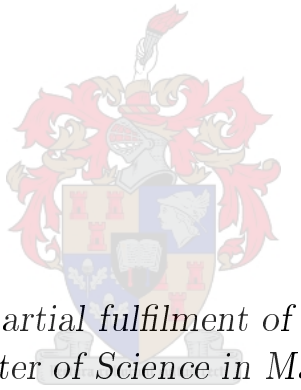
Formalizing Auctions

by

Rojo Fanamperana Randrianomentsoa



Thesis presented in partial fulfilment of the requirements for the degree of Master of Science in Mathematics in the Faculty of Science at Stellenbosch University

Supervisor: Prof. J. W. Sanders

December 2020

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 2020/06/30

Abstract

Formalizing Auctions

R. F. Randrianomentsoa
Department of Mathematics,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Thesis: MSc (Maths)
December 2020

Auctions have proven to be an efficient economical instrument over the years. Since the advent of internet-based commerce, some of their many forms have become important. To avoid problems related to the dependence on a central entity, distribution of such an instrument is crucial. In this thesis as in general Auction Theory, we consider auctions as games. Classifying their rules in two sets, we first study their mechanisms and characterize their relative optimality. Then we present a distributed sealed-bid auction protocol and a tie-breaking mechanism for that setting.

Uittreksel

Formalisering van Veilings

("Formalizing Auctions")

R. F. Randrianomentsoa

Departement Wiskunde,
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.

Tesis: MSc (Wiskunde)

Desember 2020

Veilings is oor die jare heen 'n doeltreffende ekonomiese instrument. Sedert die koms van internetgebaseerde handel het sommige van hul vele vorme belangrik geword. Om probleme te vermy wat verband hou met die afhanklikheid van 'n sentrale entiteit, is die verspreiding van so 'n instrument van deurslaggewende belang. In hierdie tesis soos in die algemene Veilingteorie, beskou ons veilings as speletjies. Ons klassifiseer hul reëls in twee stelle, bestudeer hul meganismes en kenmerk hulle relatiewe optimiteit. Daarna bied ons 'n verspreide verseëlde bod veilingsprotokol aan en 'n breukbinding meganisme vir daardie instelling.

Acknowledgements

Firstly, I would like to express my very great appreciation to my supervisor Prof. J. W. Sanders for his invaluable guidance and continuous support throughout this research project. It has been such a privilege and honour to have him as an academic father.
Secondly, I would also like to thank my examiners Dr. G. Boxall and Dr. E. Elkind for their valuable comments and suggestions.
Thirdly, I would like to express my sincere gratitude to AIMS South Africa and NRF for this opportunity. I thank all the AIMS family for their supports.
Last but not least, I would like to thank my family (Dada sy Neny, Dada, Manankasina, Rajo sy Mick, Mahery mianakavy, Mihaja sy Andry, Mahenina, Miangola) and friends for their prayers, love and supports.

"Ek wil die Here prys en nie al sy goeie dade vergeet nie." PSALMS 103:2

Dedications

Ho an'i Dadabe, ilay naniry ny hahita,
Ho an'i Dada sy i Neny, ireo nikolokolo fatratra,
Ho an'i Rajo kely, izay iriako koa hahavita,
Ho an'i Manankasina, ilay mankahery tsy ankitsahatra.

Contents

Nomenclature

Sets

$\mathbb{I}$	Set of Items
$\mathcal{B}$	Set of Bidders
$\mathcal{F}$	Set of Valuations
$\mathcal{V}$	Valuation space
$\mathcal{M}$	Mechanism space
$\mathcal{R}$	Set of Rules

Variables

t	Time
i, j	Bidders
s	State
I	Item
m	Message
b	Number of bidders
γ	Minimum Gap
w	Number of players
a	Number of prizes

Profiles

v	Valuations/Bids
A	Allocations
p	Prices
U	Utilities

Chapter 1

Introduction

> The heart of mathematics consists of concrete examples and concrete problems. Big general theories are usually afterthoughts based on small but profound insights; the insights themselves come from concrete special cases. **Paul Halmos** [1]

An auction can be viewed as a game. Its *players* are the bidders who compete to purchase certain items. It has some *rules* and at the end an *outcome*. Most importantly, as every game should, it has a *purpose*: to "efficiently" sell or buy something. Having a clear understanding of what "efficiency" means in that context, we design the auction game to achieve it.
In designing an auction game, the description should allow us, as designer, to measure the extent to which our goal is achieved. Used in the field of Mechanism Design, a.k.a. Implementation Theory [2], we have the *strategic game form* or *extensive game form*. In the latter, a set of all possible histories, some of which mark an end, and a *player function* determining the turns capture the evolution of the game. A function defined on the set of all *terminal histories* determines the *outcome* of the game. In the former, the *outcome function* is defined on the set of *action profiles* (we always mean by profile a tuple such that each coordinate corresponds to a unique player) which then completes the definition of the game in this form. Roger Myerson used this description in [3]. He called *auction mechanism* a strategic game together with a function from the set of bidder's *type* profiles to the set of action profiles. When the actions are exactly the types themselves and the function is the identity, we have a *direct revelation mechanism*.
Describing auctions as mechanisms allows us to design the game in a way that the bidders' *Dominant* or *Nash Equilibrium* strategies yield an optimal outcome for the seller.
Consider "efficiency" in the context of an auction as relative optimality of its outcome. Then we ask: "Can this be measured using the auction mechanism alone as description?". We certainly cannot tell whether the assumptions required for an auction mechanism to yield a certain outcome hold or not by

looking at the mechanism itself. Some of them depend on the settings: where the game is played (indoor? outdoor? online?) and how (centralized? distributed?).
In the present work, we describe auction games in distributed settings. With the advent of internet-based commerce, such an auction setting became important to support node failures and to avoid a bottleneck that may arise in centralized systems. Economically, as already proved by the trends of cryptocurrencies, a shift away from a centralized entity, which has a certain power on the market, is desirable. Besides, resource allocation problems in distributed systems are dealt with auction games (see for example [4]).
For one part of our description, we follow Myerson in using strategic game forms. Similar to his direct revelation mechanism, our mechanisms are outcome functions. The difference is that in [3], the domain consists of valuations for single items and the range contains pairs of probability (for obtaining the item) and expected price profiles. Here, an outcome is a pair of allocation and price profiles, and as we shall see in Chapter 2, our description overlooks the nature of items to be auctioned. Hence the theory presented here in general applies for single and multi-item auctions. By substituting $\mathbb{R}_{\geq 0}$ with $\mathbb{R}_{\leq 0}$, it also applies to *reverse auctions* [5].
Our notion of mechanism corresponds to the one in Algorithmic Mechanism Design (survey [6]). As the name suggests, computation and communication complexity concern the mechanism designer in this area (see for example [7]). With the tools from Chapter 2, the present work explores truthful mechanisms as mathematical objects. Their properties presented in Chapter 3 provide us with insights in dealing with computational problems facing Algorithmic Mechanism Design.
The other part of our description of auction games deals with the setting. Using a model of Knowledge presented in [8], we build in the second half of Chapter 2 a framework for reasoning about the environment where the auction game is played. This gives us a more complete view of the different *forms* an auction might have.
In Chapter 4, we specifically treat sealed-bid auctions. To distribute these auctions, we follow Manuel Blum's idea of Commit/Reveal [9]. The interactions are divided in two phases: first the information is transmitted without the receiver being able to access it, and second it is revealed to and checked by this same receiver. That way, all bids are broadcast in our distributed sealed-bid auctions so that arbitrators are not needed.
As part of game designing, we deal with ties which may occur in auctions. We give a protocol for tie breaking in the distributed sealed-bid auction setting in Chapter 5. The protocol is a solution to the *Leader Election Problem* which does not need a specific *network topology* [10] such as for *Herman's Ring* [11].
The present work seems to be one of the first proper treatments of distributed auctions. Beside this, there are works like [12] and [13] which focus on bid privacy. For instance in [12], Felix Brandt proposed a cryptographic protocol for

single-item sealed-bid auctions. It uses El Gamal encryption to allow the bidders computing the auction's outcome jointly, revealing the winning bid to the winner and the seller alone. The latter feature, which our general sealed-bid auction protocol doesn't have, follows from the mathematical representation of bids as boolean vectors whose components are equal to zero apart from those corresponding to the chosen bid values.
Throughout this document, we make use of Z notation for convenience. As we shall see, we have various *states* some of which have several components. Z allows us to neatly structure complex predicates without unnecessary ordering or projections. By defining *operations* with Z, we may focus on the discrete changes of states they yield and their preconditions without having to worry about data representations or code related problems. In general for a given structure, we have the following schema:

NAME OF THE STRUCTURE

LIST OF OBSERVABLES

INVARIANTS

For detailed account on Z notation, we refer to [14] or [15].

Chapter 2

Decomposing Auctions

An auction, whether it is live in a room or online, has two particular sets of rules: one concerning the way bids are collected, another dictating how the results are computed. For some auctions such as the *sealed-bid* ones, bidding and computing the results are done in two different stages. For other auctions like the traditional *English* auction, there is a sequence of temporary results changing after each bid. However, in general, these results are computed using the same function which we refer to as the *mechanism*.
These two sets of rules divide our study of auctions into two parts. The first concerns mechanism design which, regardless of the setting (room or online, centralized or distributed), consists of finding a suitable rule for computing the result of an auction game to achieve certain desired outcomes. The second part covers the bid collection rules which are necessary to ensure that the conditions required in using a given mechanism are met in a given setting.
Section 2.1 starts this chapter with informal descriptions of some standard auctions and discussion of the Revenue Equivalence Theorem. In Sections 2.2 and 2.3 we discuss auction mechanism design and define our mechanism spaces of interest. In Sections 2.4 and 2.5, we discuss bid collection rules and establish a framework for studying them in a distributed setting.

2.1 Standard Auctions for a Single Item

There are many *forms* of auction used to sell several kinds of goods, contracts, rights, etc. The most common is the traditional *English* auction. Bidders are gathered in a room to compete for a certain item. One bids to start the auction, then they all try to outbid each other. The last bidder who then has the highest bid wins the item at a price equal to his bid. In a variation of the English auction, it is the auctioneer, representing the seller, who announces the price increasingly. The bidders drop out of the auction when they do not want to bid any higher. Once a bidder has dropped out, he no longer return to the competition. In this variation, often called *ascending* auction, the last

active bidder wins the item and pays the price at which the second last bidder dropped out. Therefore, it is a dominant strategy for a bidder to stay in the competition until his valuation is exceeded, in both forms. Beyond this value, he has a negative payoff.

The standard *Dutch* auction is similar to the latter. The auctioneer starts with a reasonably high bid (as elaborated in Section 2.3) and decreases the price periodically. The first bidder to stop the clock and accept to buy the item at that price wins. It means that only one person bids and concludes the auction. Hence when the announced price reaches a bidder's valuation, he has to choose between accepting it with the possibility of winning at a lower price or waiting for it to drop with the possibility of losing. In other words, there is no dominant strategy in this auction game. Historically, this *form* of auction has been designed in order to sell tulip flowers to the highest bidder and in a short amount of time in the Netherlands.

A family of auction *forms* where bidding does not involve any (legal) interaction between the bidders is the family of sealed-bid auctions. The bids are submitted in sealed envelops which are opened only at the end. Assuming no ties, the highest bidder wins the item in all of these auctions but the price he pays varies. For instance, in *First-Price Sealed-Bid* (FPSB) auctions, he pays his own bid whereas in *Second-Price Sealed-Bid* (SPSB) auctions, he pays the second highest.

In [16], William Vickrey noted that the dilemmas facing the bidders in traditional sealed-bid (referring to FPSB) and Dutch auctions are the same. Each bidder also has to choose between bidding high with the possibility of winning at a lower price or bidding low with the possibility of losing, in FPSB. Inspired by this similarity, Vickrey introduced the SPSB auction, a "sealed" version of the ascending auction. Indeed, it is a dominant strategy for a bidder to bid his valuation in SPSB since bidding lower would only decrease his chance of winning and bidding higher might yield a payment above his valuation. The pairs FPSB-Dutch and SPSB-ascending auctions are often qualified as *strategically equivalent*.

Considering the two pairs, Vickrey analysed the expected revenue that each of these strategic games yields. It turns out that if the bidders' valuations are drawn from a uniform distribution and if they play in equilibrium, then the expected revenue is the same for these auctions. Several variations of this Revenue Equivalence Theorem have risen in the literature (survey in [17]) and most of them follow from these strategic equivalences.

While this way of studying auctions consists of analysing some given auction games, it is the inverse of the Mechanism Design problem which we discuss in the next two sections.

2.2 One Time Bidding Games

To understand the behaviour of the players (the bidders), we describe auction games in this section as one time bidding games.
Previously, we described examples of auction game in the simple case of a single item. Other cases include multiple identical items and combinatorial auctions (survey in [18]). In the former, bidders bid for blocks of these items while in the latter, they bid for bundles of complementary items. In general, the bidders are given multiple choices which, overlooking their nature, we will still refer to as *items*. Denoting the set of *items* in an auction by $\mathbb{I}$, we now understand that the bidders bid for elements of $\mathbb{I}$.
Suppose we have a finite set $\mathcal{B}$ of bidders in an auction for a finite set $\mathbb{I}$ of items. Denote by b the cardinality of $\mathcal{B}$.
Prior to bidding, each bidder $i : \mathcal{B}$ obtains random information (a.k.a. signals) concerning these items and evaluates each element of $\mathbb{I}$. Through that step, i defines a function v_i from $\mathbb{I}$ to $\mathbb{R}_{\geq 0}$ which is then the realization of a certain random variable, following a distribution over the set $\mathcal{F} := \mathbb{I} \to \mathbb{R}_{\geq 0}$. In contrast with *general* Auction Theory which deals with the random variables and their distributions (see for examples [16], [3] and [19]), we focus on subsets of $\mathcal{F}$ which contain the supports of these distributions. Specifically, we work on sets of functions, to which the actual valuation profile

$$\begin{aligned} v : \mathcal{B} &\to \mathcal{F} \\ i &\mapsto v_i \end{aligned}$$

belongs.
One key component of the auction that each bidder should be aware of prior to bidding is the *mechanism* M. Given a valuation profile v, M determines the *outcome* of the auction game which consists of an *allocation profile*

$$\begin{aligned} A :\mathcal{B} &\to \mathbb{I}_\perp \\ i &\mapsto A_i \end{aligned}$$

with $\mathbb{I}_\perp := \mathbb{I} \cup \{\perp\}$, and a *price profile*

$$\begin{aligned} p :\mathcal{B} &\to \mathbb{R}_{\geq 0} \\ i &\mapsto p_i. \end{aligned}$$

The value A_i indicates the item allocated to bidder i and $A_i = \perp$ means that i wins nothing. For the allocation A_i (even if it is equal to $\perp$), i has to pay the price p_i which may contain entrance fee, tax or fraction of his bid as in *All-Pay* auctions (see [20]). Note that the A_i's can be all equal to $\perp$ if the seller's *reserve price* is not reached in which case he keeps the items unsold.
To avoid "double selling", the allocation profile must satisfy certain conditions. In the case of multiple identical items, the total number of items allocated to

the bidders should not exceed the number of items to be sold. In combinatorial auctions, two bundles allocated to different bidders should be disjoint. In general, the feasibility of an allocation profile depends on the resource and the nature of the items. Let $\mathcal{A}$ denote the set of *feasible* allocations. Then, the mechanism M can be represented as a partial function:

$$M : (\mathcal{B} \to \mathcal{F}) \nrightarrow OUTCOME,$$

where $OUTCOME$ consists of a pair of a feasible allocation and a price per bidder.

$$\begin{array}{|l} OUTCOME \\ \hline A : \mathcal{A} \\ p : \mathcal{B} \to \mathbb{R}_{\geq 0} \\ \hline \end{array}$$

Informed about the mechanism M, every bidder i makes a bid $v_i' : \mathcal{F}$. Following the *Revelation Principle* [3], we can assume that the mechanism M is designed in a way that each bidder i is expected to report his valuation v_i. However, i's individual goal is to *win* certain valuable items in the auction at *low cost*. Therefore, i rather chooses a bid v_i' in the set $\mathcal{V}_i \subseteq \mathcal{F}$ of bids available to him, instead of v_i. To make a better choice, i measures his gain from each possible value of M then computes the set of optimal bids.
If i is allocated an item $A_i : \mathbb{I}$ and owes a price $p_i : \mathbb{R}_{\geq 0}$ for it, his gain is the difference between his value $v_i(A_i)$ for the item and p_i. This can be represented as a function U_i called *utility*:

$$\begin{aligned} U_i : \mathcal{F} \times \mathbb{I} \times \mathbb{R}_{\geq 0} &\to \mathbb{R} \\ (v_i, A_i, p_i) &\mapsto v_i(A_i) - p_i. \end{aligned}$$

Since the items allocated to the bidders are somehow related, it is convenient to capture the utilities across bidders by a *utility profile*

$$\begin{aligned} U : \mathcal{B} &\to ((\mathcal{B} \to \mathcal{F}) \times \mathcal{A} \times (\mathcal{B} \to \mathbb{R}_{\geq 0}) \to \mathbb{R}) \\ i &\mapsto ((v, A, p) \mapsto U_i(v_i, A_i, p_i)) . \end{aligned}$$

Note that some bidders may have a different meaning of the word "gain" in reality but for our study, we assume the one proposed above.

Definition 2.2.1 *A strategic game is a triple $\langle \mathcal{B}, (\mathcal{V}_{a,i})_{i:\mathcal{B}}, u \rangle$ where $\mathcal{B}$ is a set of players, $\mathcal{V}_{a,i}$ is the set of actions player i may take and $u : \prod_{i:\mathcal{B}} \mathcal{V}_{a,i} \to \mathbb{R}^b_{\geq 0}$ is a utility profile defined on the set of action profiles.*

Definition 2.2.2 *A strategic game form with consequences in a set C of outcomes is a triple $\langle \mathcal{B}, (\mathcal{V}_{a,i})_{i:\mathcal{B}}, M \rangle$ where $\mathcal{B}$ is a set of players, $\mathcal{V}_{a,i}$ is the set of actions player i may take and M is a function defined on the set of action profiles which takes its values in C.*

Remark 2.2.3 *According to Definition 2.2.1 and Definition 2.2.2 (which are from [2]), given a strategic auction game form* $\langle \mathcal{B}, (\mathcal{V}_{a,i})_{i:\mathcal{B}}, M \rangle$ *(where* $\mathcal{V}_{a,i}$ *is the set of available bids for* i *and* M *is the auction mechanism) and a valuation profile* $v : \mathcal{B} \to \mathcal{F}$*, we obtain the strategic auction game* $\langle \mathcal{B}, (\mathcal{V}_{a,i})_{i:\mathcal{B}}, u \rangle$ *where for all* $v^0 : \mathcal{B} \to \mathcal{F}$ *such that for all* $i : \mathcal{B}$*,* $v_i^0 \in \mathcal{V}_{a,i}$*,*

$$u_i(v_0^0, \cdots, v_{b-1}^0) := U_i(v, M(v^0)).$$

Since the outcome depends on the entire *bid profile*, each bidder $i : \mathcal{B}$ needs to consider the other's strategies in deducing his optimal bids. The issue is that i does not know the exact valuations nor the available bids of his opponents. What we assume he observes are subsets $(\mathcal{V}_{i,j})_{j:\mathcal{B}\setminus\{i\}}$ of $\mathcal{F}$ containing their valuations and available bids. In other words, i does not have the exact description of the strategic auction game they are playing but he has a strategic auction game form from which he can deduce games whose common set of action profiles contains the one of the actual game.
For any $v : \mathcal{B} \to \mathcal{F}$, we denote by v_{-i} the function

$$\begin{aligned} \mathcal{B} \setminus \{i\} &\to \mathcal{F} \\ j &\mapsto v_j. \end{aligned}$$

Conversely, for any $v_{-i} : \mathcal{B} \setminus \{i\} \to \mathcal{F}$ and any $v_i' : \mathcal{F}$, we denote by (v_i', v_{-i}) the function

$$\begin{aligned} \mathcal{B} &\to \mathcal{F} \\ j &\mapsto \begin{cases} v_{-i,j} & \text{if } j \neq i \\ v_i' & \text{if } j = i. \end{cases} \end{aligned}$$

Since $v^0 \mapsto U_i(v_i, v_{-i}, M(v^0))$ does not depend on v_{-i}, bidder i only needs to consider one game corresponding to, say, $v = (v_i, v_{-i})$ with certain

$$v_{-i} : \mathcal{B} \setminus \{i\} \to \mathcal{F}$$

such that for all $j \neq i$, $v_{-i,j} \in \mathcal{V}_{i,j}$. Therefore, he obtains an optimal bid by maximizing

$$v^0 \mapsto U_i(v, M(v^0))$$

over the product

$$\prod_{j:\mathcal{B}} \mathcal{V}_{i,j} := \{v^0 : \mathcal{B} \to \mathcal{F} \mid \forall\, j : \mathcal{B} \bullet v_j^0 \in \mathcal{V}_{i,j}\}$$

where $\mathcal{V}_{i,i} = \mathcal{V}_{a,i}$ is the set of available bids for i.
An alternative in Auction Theory, to address the issue of bidders not knowing each other's valuation, is to assume that the random variables giving these valuations have distributions that are "known" to the bidders. Following [21],

if a bidder studies some of his potential competitors' *bidding patterns* in previous auctions, he can define an "average" probability distribution for them. Having the game defined this way, he maximizes his *expected utility* instead of maximizing the function over his set of available bids. From the designer's perspective, it would be unrealistic to assume that all bidders in a distributed auction would find the same probability distribution for their respective opponents.

2.3 Mechanism Design

Given that the bidders would behave as described in Section 2.2 during an auction game, the auctioneer should design a strategic auction game form whose mechanism M would be *fair* for them and would guarantee maximum profit to the seller at the same time.
First, the auctioneer should consider each bidder's valuation. The set of available bid profiles must contain the actual valuation profile which, as mentioned in Remark 2.2.3, will determine the strategic auction game to be played. Like every bidder, the auctioneer does not know the exact valuation profile but he can always choose a subset

$$\mathcal{V} \subseteq \mathcal{B} \to \mathcal{F}$$

that is *big enough* to contain it. He then defines M on this set which we call the *valuation space*.
For instance, in a single-item Dutch auction, the valuation space can be the product of b copies of a finite list of values; the maximum of these being higher than the maximum valuation of the bidders. In general, $\mathcal{V}$ is not necessarily *symmetric* as in that example (by *symmetry*, we mean $\mathcal{V}_i = \mathcal{V}_j$ for all $i, j : \mathcal{B}$). However, assuming symmetry is more practical in the case of a large number of bidders. Valuation space will be further discussed in Chapter 3.
When defining the mechanism M, a criterion the auctioneer needs to respect is that every bidder should have non-negative utility by reporting his valuation in the auction. Therefore, he considers only mechanisms which satisfy $U_i(v, M(v)) \geq 0$ for all $v : \mathcal{V}$ and for all $i : \mathcal{B}$. Formally, the *mechanism space* which is the set of mechanisms he considers in his design, must be contained in the set

$$\mathcal{M}(\mathcal{V}) := \{M : \mathcal{V} \to OUTCOME \mid \forall\, v : \mathcal{V}, \forall\, i : \mathcal{B} \bullet U_i(v, M(v)) \geq 0\}.$$

Since every bidder i would maximize his utility while he is expected to report his true valuation v_i, the auctioneer should choose a mechanism in which v_i would be an optimal bid for i. We qualify such a mechanism as being *truthful* or *incentive compatible* [6], [3].
For instance, the SPSB auction offers an option for selling a single item. The

mechanism used in this auction allocates the item to the highest bidder who then pays the runner up's bid. Therefore, the only bid that would maximize the bidder's utility is exactly his valuation v_i unless he colludes with the others. Note that if the bidders communicate their strategies to each other before the auction, they can manipulate the bids together in a way that the winning bidder pays a lower price than the real second highest bid and share the surplus. To avoid such an event, the auctioneer can simply restrict the mechanism space to the set

$$\mathcal{M}^u(\mathcal{V}) := \{M : \mathcal{M}(\mathcal{V}) \mid \forall\, v : \mathcal{V}, \forall\, i : \mathcal{B} \bullet v \in \arg max\ v' \mapsto U_i(v, M(v'))\}.$$

Note that here, v is not required to be the only value for which the maximum is reached. And in general throughout this document, $\arg max\, f$ is rather a non-empty subset of $\operatorname{dom} f$ than a single element.
If an auction game implements such a mechanism, then the players (individually and also collectively) have incentive to bid their true valuations assuming that they are only interested in maximizing their own utilities and not in hiding their valuations at any cost or in minimizing one another's utilities. Observe that if

$$\cap_{i:\mathcal{B}} \arg max\ v' \mapsto U_i(v, M(v'))$$

has two or more elements and if the players use v^0 in this intersection that is not the actual valuation profile v, then each bidder obtains the same utility as he would for v.
Another alternative for the auctioneer is to assume *independence*. This is allowed only because the bids can be made anonymous in online auctions and the number of bidders on platforms like eBay is large enough. We say that two bidders i and j are *independent* if and only if neither of them is certain about the other's valuation nor bid.
Assuming that the bidders are mutually independent, the auctioneer should design the auction mechanism in a way that unilateral deviation from truthful bidding would make the bidder worse off. In other words, he should consider auction games in which the actual valuation profile is a *pure Nash equilibrium* point. Denote by

$$\mathcal{M}^N(\mathcal{V}) := \{M : \mathcal{M}(\mathcal{V}) \mid \forall\, v : \mathcal{V}, \forall\, i : \mathcal{B} \bullet v_i \in \arg max\ v_i' \mapsto U_i(v, M(v_i', v_{-i}))\}$$

the set of such mechanisms.
Finally, assuming that the bidders would report their true valuation, the auctioneer should find a mechanism which maximizes the total value of the allocations across bidders. Considering the function

$$\begin{aligned} \Psi :\ & \mathcal{V} \times \mathcal{A} \to \mathbb{R}_{\geq 0} \\ & (v, A) \mapsto \sum_{i:\mathcal{B}} v_i(A_i), \end{aligned}$$

the mechanism space should be contained in

$$\mathcal{M}^s(\mathcal{V}) := \{M : \mathcal{M}(\mathcal{V}) \mid \forall\, v : \mathcal{V} \bullet M(v).A \in \arg\, max\ A \mapsto \Psi(v, A)\}.$$

Note that the assumption about truthful bidding has allowed the auctioneer to use such mechanisms to maximize the total value. If the bidders lie about their valuations, the total value would be different. Imagine a single item FPSB auction with 2 bidders i and j. If i values the item at \$400 and j values it at \$300 but they respectively bid \$250 and \$270, then the mechanism awards the item to j which means that the allocation made a total value of \$300. Although the mechanism of a *FPSB* auction awards the item to the highest bidder, which means that it is in $\mathcal{M}^s(\mathcal{V})$, the maximum total value (which is equal to \$400) is not achieved since the bidders did not report their true value for the item.
For the rest of this document, except Chapter 3, we assume that the valuation space $\mathcal{V}$ is the product

$$\prod_{i:\mathcal{B}} \mathcal{V}_i := \{v : \mathcal{B} \to \mathcal{F} \mid \forall\, i : \mathcal{B} \bullet v_i \in \mathcal{V}_i\}$$

where the $\mathcal{V}_i$'s are fixed subsets of $\mathcal{F}$.

2.4 Bid Collection Rules

In Sections 2.2 and 2.3, we assumed that each bidder i observes a collection $(\mathcal{V}_{i,j})_{j:\mathcal{B}\setminus\{i\}}$ of subsets of $\mathcal{F}$ containing the true valuations and available bids of his opponents. This assumption enabled us to define a strategic auction game form which has helped in understanding Mechanism Design. However, as mentioned in the first paragraph of this chapter and as the examples of Section 2.1 demonstrate, an auction is not a single input/output of the mechanism. In each of these examples, the protocol for collecting the bids is described, for it is as important as the mechanism. The interactions between the bidders and the auctioneer or between the bidders themselves provide them with new information they can use during the auction. Therefore, the choice of protocol should match the choice of mechanism to ensure truthful bidding. For instance, if the mechanism is designed for *independent* bidders, then the protocol should not involve interactions that would change this property during bidding. To analyse such kind of properties in a "dynamical" setting, we need to formalize first the bid collection rules, then the properties in question.
Following the previous sections, each bidder $i : \mathcal{B}$ initially has a valuation $v_i : \mathcal{V}_i$ and a set $\mathcal{V}_{a,i} \subseteq \mathcal{V}_i$ of available bids. As the auction evolves, v_i or $\mathcal{V}_{a,i}$ might change. Consider for example a bidder i who valued a bundle of violin and bow for \$10,000 at the beginning of a five-day auction on eBay then on the second day, got an acceptable bow from a different source. If his intention

was to have exactly the violin and one bow, his new valuation for the set would be lower than the initial one. This example is indeed personal but confirms the possibility of v_i changing. It is possible that the bidder simply learned more about the item during the auction and changed his valuation. For the set $\mathcal{V}_{a,i}$, we can consider a single-item English auction. Once a bidder j bids v'_j, any smaller bid $v'_i : \mathcal{V}_{a,i}$ is no longer available hence should be removed from the set.
In general, there are two ways for communicating the bids: either through the auctioneer or directly to every other participant (auctioneer/seller and bidders). Here we opt for the second, to avoid the auctioneer manipulating the results. In an auction room, this can mean that the bids are called out or in the case of Sealed-bid auctions, revealed in front of the bidders. For online auctions, we assume that the bids are broadcast in a message of type *OMES* which contains the bidder's identity *id* and the bid *oBid*. Note that the letter *"O"* preceding "MES" (short for "message") means "open". The reason for this emphasis will be made clear in Chapter 4.

OMES

$$id : \mathcal{B}$$
$$oBid : \mathcal{F}$$

As we consider distributed auctions, we assume that each bidder i records the bids he has received or sent in a set $oRec_i : \mathbb{P}\, OMES$. Moreover, to complete our view of the global state of an auction, we observe an additional (external) set $aoRec : \mathbb{P}\, OMES$ which contains all messages of type *OMES* broadcast in the system.

State$[\mathcal{V}]$

$$v : \mathcal{B} \to \mathcal{F}$$
$$\mathcal{V}_a : \mathcal{B} \to \mathbb{P}\, \mathcal{F}$$
$$oRec : \mathcal{B} \to \mathbb{P}\, OMES$$
$$aoRec : \mathbb{P}\, OMES$$

$$\forall\, i : \mathcal{B} \bullet v_i \in \mathcal{V}_i \land \mathcal{V}_{a,i} \subseteq \mathcal{V}_i$$

As captured by the invariant of this schema, the set $\mathcal{V}_{a,i}$ of available bids must be contained in the projection $\mathcal{V}_i$ of the valuation space while the valuation v_i may be more general. For instance in a single-item Dutch auction, v_i is not available until the announced price reaches this value.
At the base of what follows are propositions concerning $s.v_i$, $s.\mathcal{V}_{a,i}$, $s.oRec_i$ and $s.aoRec$ for all $i : \mathcal{B}$ and $s : State[\mathcal{V}]$.
At this point, we can define any auction by a mechanism *aM* and a sequence

$aS : \operatorname{seq} State[\operatorname{dom} aM]$ of global states satisfying a certain set of rules. Although we assume that the states change only in finite time, we let aS be an infinite sequence for there is no fixed upper bound. Modelling *Time* by the set $\mathbb{Z}$, we can assume that bidding starts at certain time t^0 before which advertising and registrations take place. However, as we focus on the changes of states occurring during the auction, we assume for simplicity that bidding starts at time $t = 0$ and consider the set $\mathbb{N}$ instead.
The auction *form* determines the rules which the sequence aS must follow. However, some of these rules are common to all *forms* of auction.
Firstly, there is no sent message in the initial state $aS[0]$:

$$R_0(aS) := aS[0].aoRec = \{\}.$$

Secondly, a message received by a bidder i must have been broadcast:

$$R_1(aS) := \forall\, t : \mathbb{N}, \forall\, i : \mathcal{B} \bullet aS[t].oRec_i \subseteq aS[t].aoRec.$$

Note that R_0 and R_1 imply that $aS[0].oRec_i = \{\}$ for all $i : \mathcal{B}$.
Thirdly, sending and receiving cannot be undone. Any message broadcast or received by i at $t : \mathbb{N}$ has been respectively broadcast or received by i at any later time $t' \geq t$.

$$R_2(aS) := \forall\, t^0, t^1 : \mathbb{N} \bullet (t^0 < t^1) \Rightarrow (aS[t^0].aoRec \subseteq aS[t^1].aoRec),$$
$$R_3(aS) := \forall\, t^0, t^1 : \mathbb{N}, \forall\, i : \mathcal{B} \bullet (t^0 < t^1) \Rightarrow (aS[t^0].oRec_i \subseteq aS[t^1].oRec_i).$$

Lastly, a bidder i cannot submit a bid v_i' unless it is available to him. Therefore, if a message $m : OMES$ is broadcast, $m.oBid$ must have been available to the bidder which we qualify by calling that bid *valid*.

$$\begin{aligned} R_4(aS) := &\forall\, t^0 : \mathbb{N}, \forall\, m : aS[t].aoRec, \exists\, t^1 \leq t^0 \bullet \\ &(i = m.id) \Rightarrow (m.oBid \in aS[t^1].\mathcal{V}_{a,i}). \end{aligned}$$

An auction *form* is given by a mechanism M defined on a valuation space $\mathcal{V}$ and a set $\mathcal{R}$ of rules containing $\{R_k \mid k \in [0, 4]\}$. An auction of the form $(M, \mathcal{R})$ is composed of the mechanism M and a sequence $aS : \operatorname{seq} State[\mathcal{V}]$ of states satisfying the rules in $\mathcal{R}$.

$AUC[(M, \mathcal{R})]$

$aM : \mathcal{M}(\mathcal{V})$
$aS : \operatorname{seq} State[\mathcal{V}]$

$aM = M$
$\forall\, R : \mathcal{R} \bullet (R(aS)) = \text{true}$

2.5 Who Knows What When?

As mentioned in Section 2.4, some sets of bid collection rules allow the bidders to acquire new information they can use during the game. For instance in an English auction for single-item, each bidder *knows* it when he receives a message. Consequently, he knows that the corresponding bid is valid and assuming that the bidders always receive a particular message at the same time, he *knows* that any smaller bid is no longer available for any of his opponents. To formalize this intuition as well as similar properties, we use Epistemic and Temporal Logics [8].
When we defined $State[\mathcal{V}]$ in Section 2.4, we described three elements that are local to each bidder i, namely his valuation v_i, his set $\mathcal{V}_{a,i}$ of available bids and the set $oRec_i$ of the messages he has received. Consider the equivalence relation

$$\begin{aligned} &s^0 \sim_i s^1 \text{ if and only if} \\ &(s^0.v_i = s^1.v_i) \wedge (s^0.\mathcal{V}_{a,i} = s^1.\mathcal{V}_{a,i}) \wedge (s^0.oRec_i = s^1.oRec_i) \end{aligned}$$

on $State[\mathcal{V}]$ for all $i : \mathcal{B}$. Each of these induces an equivalence relation on $AUC[(M, \mathcal{R})] \times \mathbb{N}$. Specifically,

$$(auc^0, t^0) \sim_i (auc^1, t^1) \text{ if and only if } auc^0(t^0) \sim_i auc^1(t^1).$$

Following the semantics given in Chapter 4 of [8], we consider the *structure*

$$\mathcal{K}(M, \mathcal{R}) := (AUC[(M, \mathcal{R})] \times \mathbb{N}, \pi, (\sim_i)_{i:\mathcal{B}}),$$

where $\pi(auc, t)(P)$ is the *interpretation* (true or false) at the point $(auc, t) : AUC[(M, \mathcal{R})] \times \mathbb{N}$ of proposition P concerning valuations or available bids or bid messages in state $s : State[\mathcal{V}]$. We define π by

$$\pi(auc, t)(P) := P(auc.aS[t]),$$

and write:

(D_0) $(\mathcal{K}(M, \mathcal{R}), auc, t) \vDash P$ if and only $\pi(auc, t)(P) = \text{true}$,

(D_1) $(\mathcal{K}(M, \mathcal{R}), auc, t) \vDash \varphi \wedge \varphi'$ if and only if

$$(\mathcal{K}(M, \mathcal{R}), auc, t) \vDash \varphi \wedge (\mathcal{K}(M, \mathcal{R}), auc, t) \vDash \varphi',$$

(D_2) $(\mathcal{K}(M, \mathcal{R}), auc, t) \vDash \neg\, \varphi$ if and only if $(\mathcal{K}(M, \mathcal{R}), auc, t) \nvDash \varphi$.

For a proposition φ, we say that bidder i *knows* φ at a point $(auc^0, t^0) : AUC[(M, \mathcal{R})] \times \mathbb{N}$ and write

$$(\mathcal{K}(M, \mathcal{R}), auc^0, t^0) \vDash K_i\varphi,$$

if and only if φ holds at any equivalent point (auc^1, t^1) to i.

(D_3) $(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_i\varphi$ if and only if

$$\forall (auc^1, t^1) \sim_i (auc^0, t^0) \bullet (\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \vDash \varphi.$$

Before continuing with auction games, let us examine the *S5 Properties* [8] for our definition of *Knowledge*.

- *Knowledge Axiom*: Since the relation $\sim_i$ is reflexive, (D_3) implies that

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_i\varphi \Rightarrow (\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash \varphi.$$

  This means that if bidder i knows φ, then φ is true.

- *Positive Introspection Axiom*: Suppose

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_i\varphi,$$

  and let $(auc^1, t^1) \sim_i (auc^0, t^0)$. From the transitivity of $\sim_i$, any (auc^2, t^2) equivalent to (auc^1, t^1) is also equivalent to (auc^0, t^0). Hence, we have

  $$(\mathcal{K}(M,\mathcal{R}), auc^2, t^2) \vDash \varphi,$$

  for all $(auc^2, t^2) \sim_i (auc^1, t^1)$ which means that

  $$(\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \vDash K_i\varphi.$$

  Since (auc^1, t^1) is arbitrary, we have

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_iK_i\varphi.$$

  This shows that if bidder i knows φ, then he knows that he knows φ.

- *Negative Introspection Axiom*: Suppose

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash \neg\, K_i\varphi.$$

  By (D_2) and (D_3), it means that there exists $(auc^1, t^1) \sim_i (auc^0, t^0)$ such that

  $$(\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \nvDash \varphi.$$

  Let $(auc^2, t^2) \sim_i (auc^0, t^0)$. By symmetry and transitivity of $\sim_i$, we obtain $(auc^0, t^0) \sim_i (auc^1, t^1)$ and $(auc^2, t^2) \sim_i (auc^1, t^1)$. Therefore,

  $$(\mathcal{K}(M,\mathcal{R}), auc^2, t^2) \vDash \neg\, K_i\varphi,$$

  and since (auc^2, t^2) is arbitrary,

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_i\neg\, K_i\varphi.$$

  In words, if a bidder i does not know φ, then he knows that he does not know φ.

- *Knowledge Generalization Rule*: Assume that

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash \varphi,$$

  for all $(auc^0, t^0) : AUC[(M,\mathcal{R})]\times\mathbb{N}$ and let $(auc^1, t^1) : AUC[(M,\mathcal{R})]\times\mathbb{N}$. For any $(auc^2, t^2) \sim_i (auc^1, t^1)$, we have

  $$(\mathcal{K}(M,\mathcal{R}), auc^2, t^2) \vDash \varphi.$$

  Hence,

  $$(\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \vDash K_i\varphi.$$

  This means that if φ is true at any point of $AUC[(M,\mathcal{R})]\times\mathbb{N}$, then any bidder i knows φ at any of these points.

- *Consequence Axiom*: Suppose

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_i\varphi \wedge K_i(\varphi \Rightarrow \varphi').$$

  It follows from (D_1) and (D_3) that

  $$(\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \vDash \varphi \text{ and } (\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \vDash (\varphi \Rightarrow \varphi'),$$

  for all $(auc^1, t^1) \sim_i (auc^0, t^0)$. Thus, we have

  $$(\mathcal{K}(M,\mathcal{R}), auc^1, t^1) \vDash \varphi',$$

  for all $(auc^1, t^1) \sim_i (auc^0, t^0)$ which means that

  $$(\mathcal{K}(M,\mathcal{R}), auc^0, t^0) \vDash K_i\varphi'.$$

  Therefore, if a bidder i knows φ and in addition he knows that φ' is a consequence of φ, then he also knows φ'.

Looking back at our intuition for single-item English auctions $Eng := (M_E, \mathcal{R}_E)$, as described in the first paragraph of this section, if we substitute "no longer" with "not", the property can be written as follows. If a bidder i records a bid message m at point (auc^0, t^0), the he knows he received m. Consequently, he knows that $m.oBid$ is valid (m is in $auc^0.aS[t^0].aoRec$) and that any bid v_j' smaller than $m.oBid$ is not in $auc^0.aS[t^0].\mathcal{V}_{a,j}$ for all $j : \mathcal{B}$, assuming the bidders always receive a particular message at the same time. Consider the propositions

$$P^0(s) := m \in s.oRec_i,$$
$$P^1(s) := m \in s.aoRec,$$
$$P^2(s) := \forall j : \mathcal{B}, \forall\, v_j' \leq m.oBid \bullet v_j' \notin s.\mathcal{V}_{a,j}.$$

Then the following proposition formally states the property we discussed above.

Proposition 2.5.1 *Let $i : \mathcal{B}$ and $m : OMES$. Then*

$$(\mathcal{K}(Eng), auc^0, t^0) \vDash P^0 \Rightarrow (\mathcal{K}(Eng), auc^0, t^0) \vDash K_iP^0,$$
$$(\mathcal{K}(Eng), auc^0, t^0) \vDash K_iP^0 \Rightarrow (\mathcal{K}(Eng), auc^0, t^0) \vDash (K_iP^1 \wedge K_iP^2).$$

***Proof*:** By the definition of $\sim_i$ and (D_3), $K_i P^0$ holds whenever P^0 does.

$$\left((\mathcal{K}(Eng), auc^0, t^0) \vDash P^0 \Rightarrow (\mathcal{K}(Eng), auc^0, t^0) \vDash K_i P^0\right).$$

Besides, as mentioned in Section 2.4, $R_1 \in \mathcal{R}_E$. Therefore, R_1 is satisfied at every point $(auc^1, t^1) \in AUC[Eng] \times \mathbb{N}$ (meaning that $R_1(auc^1.aS)$ holds) and $auc^1.aS[t^1].oRec_i$ is included in $auc^1.aS[t^1].aoRec$. Hence

$$(\mathcal{K}(Eng), auc^1, t^1) \vDash (P^0 \Rightarrow P^1),$$

for all $(auc^1, t^1) \in AUC[Eng] \times \mathbb{N}$. Applying the Knowledge Generalization Rule,

$$(\mathcal{K}(Eng), auc^1, t^1) \vDash K_i(P^0 \Rightarrow P^1),$$

for all $(auc^1, t^1) \in AUC[Eng] \times \mathbb{N}$, and particularly for $(auc^1, t^1) = (auc^0, t^0)$. From the Consequence Axiom, we conclude that

$$(\mathcal{K}(Eng), auc^0, t^0) \vDash K_i P^1.$$

Note that since R_1 is part of every auction form, this property holds for them too.
For the last term of the second inference in our statement, we need to formalize a proper rule of the single-item English auction. As described in Section 2.1, the bids in a single-item English auction are increasing. Therefore, when a bidder receives a bid v_j', any smaller bid is no longer available for him.

$$\begin{aligned} R_{E,0}(aS) :=& \forall\, t^1 : \mathbb{N}, \forall\, j : \mathcal{B} \bullet \\ & m \in aS[t^1].oRec_j \Rightarrow \forall\, t^2 \geq t^1, \forall\, v_j' \leq m.oBid \bullet v_j' \notin aS[t^2].\mathcal{V}_{a,i}. \end{aligned}$$

The assumption that every bidder receives a message at the same time, can be written as follows:

$$\forall\, t^1 : \mathbb{N}, \forall\, i, j : \mathcal{B} \bullet m \in aS[t^1].oRec_i \Leftrightarrow m \in aS[t^1].oRec_j.$$

Therefore, if P^0 holds at $auc^1.aS[t^1]$, then $m \in auc^1.aS[t^1].oRec_j$ for all $j : \mathcal{B}$. Hence, $R_{E,0}$ implies that P^2 holds at $auc^1.aS[t^1]$. Thus,

$$(\mathcal{K}(Eng), auc^1, t^1) \vDash (P^0 \Rightarrow P^2),$$

for all $(auc^1, t^1) \in AUC[Eng] \times \mathbb{N}$. Using the Knowledge Generalization Rule, we obtain

$$(\mathcal{K}(Eng), auc^0, t^0) \vDash K_i(P^0 \Rightarrow P^2).$$

Again, we conclude from the Consequence Axiom.

□

Recall that before we formalized the latter property, we changed "no longer" into "not". In order to express our original statement and other properties of auction games, we consider the temporal operators: $\Box$ (*always*), $\Diamond$ (*eventually*), $\bigcirc$ (*next time*) and $\mathbf{U}$ (*until*). We say that $\bigcirc\varphi$ is true if φ is true at the next step and $\varphi \mathbf{U} \varphi'$ is true if φ is true until φ' is true. Following [8], we give the subsequent definitions.

(D_4) $(\mathcal{K}(M,\mathcal{R}), auc, t) \vDash \bigcirc\varphi$ if and only $(\mathcal{K}(M,\mathcal{R}), auc, t+1) \vDash \varphi$.

(D_5) $(\mathcal{K}(M,\mathcal{R}), auc, t^0) \vDash \varphi \mathbf{U} \varphi'$ if and only if there exists $t^1 \geq t^0$ such that

$$(\mathcal{K}(M,\mathcal{R}), auc, t^1) \vDash \varphi',$$

and for all $t^2 : \mathbb{N}$,

$$t^0 \leq t^2 < t^1 \Rightarrow (\mathcal{K}(M,\mathcal{R}), auc, t^2) \vDash \varphi.$$

For a proposition φ, $\Diamond\varphi$ (φ is true in the future) is equivalent to (true $\mathbf{U}\varphi$) and $\Box\varphi$ (φ is true now and at any later time) is equivalent to the dual $\neg \Diamond \neg \varphi$. As the sentence "any smaller bid is *no longer* available" literary means "any smaller bid is always not available", we now substitute $K_i P^2$ with $K_i(\Box P^2)$. The definition of $R_{E,0}$ allows us to adjust our reasoning and obtain the statement in the first paragraph of this section. Hence we have the following proposition.

Proposition 2.5.2 *Let* $(auc, t) : AUC[Eng] \times \mathbb{N}$, $i : \mathcal{B}$ *and* $m : OMES$. *Then,*

$$(\mathcal{K}(Eng), auc, t) \vDash P^0 \Rightarrow (\mathcal{K}(Eng), auc, t) \vDash K_i(\Box P^2).$$

2.6 Chapter Summary

In this chapter, we have introduced a framework for studying auction games. The decomposition of the rules into two sets allows us on one hand to study the bidders' strategies in a static and centralized view while on the other to reason about the interactions involved in a way that extends to the distributed setting.
To prepare for distributions of mechanisms, we have considered sets of valuations rather than random variables. By that approach, we can use properties of these functions to characterize truthful mechanisms in Chapter 3.
While introducing the second part of this framework, we have specifically looked at the example of a distributed English auction. We have established that in such auctions, the bidders learn about their opponents' available bids during bidding. In investigating knowledge we have used the approach of Correspondence Theory to infer laws from semantics properties. As we shall see in Chapter 4, our approach for describing bid collection rules prove to be convenient in analysing distributed auctions.

Chapter 3

Mechanism and Valuation Spaces

As mentioned in Section 2.1 to Section 2.3, our approach to studying mechanisms consists of using the properties of valuations as functions.
Since every mechanism is defined on a subset of $\mathcal{B} \to \mathcal{F}$, we can conduct our study in two complementary ways. On one side, we fix the valuation space $\mathcal{V} \subseteq \mathcal{B} \to \mathcal{F}$ then characterize the set of mechanisms defined on $\mathcal{V}$ which satisfy certain predefined properties as introduced in Section 2.3. On the other side, given a mechanism M, we discuss the domain on which certain desired property holds for M.
In this chapter, we start by giving the underlying mechanisms of the standard single-item auctions in Section 3.1. Then, we discuss the valuation space in Section 3.2. In Sections 3.3 and 3.4, we present results concerning $\mathcal{M}^s(\mathcal{V})$ and $\mathcal{M}^u(\mathcal{V})$ respectively. And in Section 3.5, we discuss the mechanism space $\mathcal{M}^N(\mathcal{V})$.

3.1 Mechanisms for Single Item Auctions

Following the decomposition of auctions as introduced in Chapter 2, any of the standard single-item auctions given in Section 2.1 uses a mechanism in the family $(M_k)_{k:\mathbb{N}^*}$ subsequently described. Let $\mathbb{I} = \{I\}$ and $p^k(v)$ the k-th maximum bid. Particularly, assuming sufficient bids, let

$$p^1(v) := max\{v_j(I) : \mathbb{R}_{\geq 0} \mid j : \mathcal{B}\},$$

and

$$p^2(v) := max\left(\{v_j(I) : \mathbb{R}_{\geq 0} \mid j : \mathcal{B}\} \setminus \{max\{v_j(I) : \mathbb{R}_{\geq 0} \mid j : \mathcal{B}\}\}\right).$$

Assuming no ties, $\arg max\{v_j(I) \mid j : \mathcal{B}\}$ is a singleton which can be identified with the bidder it contains. So we define

$$\begin{aligned} M_k : \mathcal{V} &\to OUTCOME \\ v &\mapsto M_k(v) \end{aligned}$$

by

$$M_k(v).A_i = \begin{cases} I & \text{for } i = \arg max\{v_j(I) \mid j : \mathcal{B}\} \\ \perp & \text{otherwise,} \end{cases}$$

$$M_k(v).p_i = \begin{cases} p^k(v) & \text{for } i = \arg max\{v_j(I) \mid j : \mathcal{B}\} \\ 0 & \text{otherwise.} \end{cases}$$

Note that we do not consider entrance fees or taxes (as mentioned in Section 2.2) in that definition.
For the sealed-bid auctions, it is clear from their definitions which k is used. For instance, FPSB and SPSB auctions respectively use M_1 and M_2. Since the only bidder who bids in a Dutch auction pays this bid, the underlying mechanism is M_1. For English or ascending auctions, their identification with SPSB auctions (by Vickrey) as introduced in Section 2.1 might be confusing. It is important to emphasize that the "equivalence" between them concerns the strategies in the corresponding games. Recall that we refer to the function for computing the result as a mechanism. Following the description of English auction, we have the highest bidder paying his own bid. Therefore, the mechanism used is M_1.

3.2 Valuation Space

As introduced in Section 2.3, a valuation space is a domain on which the auction mechanism is defined. In that section, we mentioned that the auctioneer can always choose one that is *big enough* to contain the profile of bidders' valuations. This freedom follows from Proposition 3.2.1 which states that if the property (among those cited in Section 2.3) he wants the mechanism to satisfy holds on a set $\mathcal{V}$, then it also holds on any subset of $\mathcal{V}$.

Proposition 3.2.1 *Let $\mathcal{V}^0 \subseteq \mathcal{V}^1 \subseteq \mathcal{B} \to \mathcal{F}$. Then,*

$$\{M_{|\mathcal{V}^0} \mid M : \mathcal{M}(\mathcal{V}^1)\} \subseteq \mathcal{M}(\mathcal{V}^0),$$
$$\{M_{|\mathcal{V}^0} \mid M : \mathcal{M}^s(\mathcal{V}^1)\} \subseteq \mathcal{M}^s(\mathcal{V}^0),$$
$$\{M_{|\mathcal{V}^0} \mid M : \mathcal{M}^u(\mathcal{V}^1)\} \subseteq \mathcal{M}^u(\mathcal{V}^0),$$
$$\{M_{|\mathcal{V}^0} \mid M : \mathcal{M}^N(\mathcal{V}^1)\} \subseteq \mathcal{M}^N(\mathcal{V}^0).$$

***Proof*:**

- Let $M : \mathcal{M}(\mathcal{V}^1)$ and let $v : \mathcal{V}^0$. Then $v \in \mathcal{V}^1$ and for all $i : \mathcal{B}$, $U_i(v, M(v)) \geq 0$. Therefore, $M_{|\mathcal{V}^0} \in \mathcal{M}(\mathcal{V}^0)$.
- Similarly, let $M : \mathcal{M}^s(\mathcal{V}^1)$ and let $v : \mathcal{V}^0$. Then $v \in \mathcal{V}^1$ and for all $i : \mathcal{B}$, $M(v).A \in \arg max\ A \mapsto \Psi(v, A)$. Therefore, $M_{|\mathcal{V}^0} \in \mathcal{M}^s(\mathcal{V}^0)$.

- Let $M : \mathcal{M}^u(\mathcal{V}^1)$, $v : \mathcal{V}^0$ and $i : \mathcal{B}$. Since $\mathcal{V}^0 \subseteq \mathcal{V}^1$, we have

$$U_i(v, M(v')) \leq U_i(v, M(v))$$

for every $v' : \mathcal{V}^0$. It follows that $v \in \arg max\, v' \mapsto U_i(v, M(v'))$ and $M_{|\mathcal{V}^0} \in \mathcal{M}^u(\mathcal{V}^0)$.

- Similarly, let $M : \mathcal{M}^N(\mathcal{V}^1)$, $v : \mathcal{V}^0$ and $i : \mathcal{B}$. Since $\mathcal{V}^0 \subseteq \mathcal{V}^1$,

$$U_i(v, M(v_i', v_{-i})) \leq U_i(v, M(v_i, v_{-i})),$$

for every $v_i' \in \mathcal{V}_i^0$. Therefore, $v_i \in \arg max\, v_i' \mapsto U_i(v, M(v_i', v_{-i}))$ and $M_{|\mathcal{V}^0} \in \mathcal{M}^N(\mathcal{V}^0)$.

□

Having Proposition 3.2.1, we might be tempted to simply consider $\mathcal{B} \to \mathcal{F}$ as valuation space. However, we are dealing with maximization problems and we need to ensure the existence of a solution, specifically an optimal mechanism M defined on this valuation space.
Note that for the space $\mathcal{M}^s(\mathcal{V})$, the maximization is over the finite set $\mathcal{A}$ of allocation profiles for a fixed valuation profile $v \in \mathcal{V}$. Therefore, the existence of such a mechanism does not depend on the non-empty set $\mathcal{V}$.
For $\mathcal{M}^u$ and $\mathcal{M}^N$, the mechanisms are solutions of the systems of inequalities

$$U_i(v, M(v).A, M(v).p) \geq U_i(v, M(v').A, M(v').p), \forall\, i : \mathcal{B}, \forall\, v, v' : \mathcal{V},$$

and

$$U_i(v, M(v).A, M(v).p) \geq U_i(v, M(v_i', v_{-i}).A, M(v_i', v_{-i}).p), \forall\, i : \mathcal{B}, \forall\, v : \mathcal{V}, \forall\, v_i' : \mathcal{V}_i,$$

respectively. Note that the constant mechanism which always allocates $\perp$ to every bidder at a price equal to zero is a solution to both systems although it is not an optimal mechanism.
Recall that $\mathcal{F}$ is the set of non-negative real-valued functions on a finite set $\mathbb{I}$ and $\mathcal{B}$ is a finite set of bidders. Therefore, we can identify $\mathcal{B} \to \mathcal{F}$ with $\mathbb{R}_{\geq 0}^{b \times \#\mathbb{I}}$ and use an induced topology from $\mathbb{R}^{b \times \#\mathbb{I}}$. Particularly, we can consider the l_1-*distance* which is the sum of the differences across coordinates. In our notation, the distance is defined by

$$d(v^0, v^1) := \sum_{i:\mathcal{B}} \sum_{I \in \mathbb{I}} \left| v_i^0(I) - v_i^1(I) \right|$$

for all $v^0, v^1 : \mathcal{B} \to \mathcal{F}$. From now on, we assume that the valuation space is a *compact* subset of the metric space $(\mathcal{B} \to \mathcal{F}, d)$.
As there are finitely many items, the range of a valuation $v_i : \mathcal{F}$ of a bidder i is finite. If it is not a singleton, then there exists a minimum distance (strictly

positive) between its elements. Fixing a lower bound for such minimum distance, we restrict our attention to valuations which assign to two different items a multiple of $2b\gamma$ for a given $\gamma > 0$. Let

$$\mathcal{F}_\gamma := \{v : \mathcal{B} \to \mathcal{F} \mid \forall\, i : \mathcal{B}, \forall\, I^0, I^1 : \mathbb{I}, \exists\, k \in \mathbb{N} \bullet \left|v_i(I^0) - v_i(I^1)\right| = 2bk\gamma\}. \tag{3.2.1}$$

For the rest of this chapter, the open balls we refer to are those of $(\mathcal{F}_\gamma, d)$, namely

$$B(v^0, r) := \{v^1 : \mathcal{F}_\gamma \mid d(v^0, v^1) < r\},$$

for $r > 0$ and $v^0 : \mathcal{F}_\gamma$.

3.3 Maximizing the Total Value

As mentioned in Section 2.3, one of the auctioneer's goals is to maximize the total true value yielded by the allocations across bidders. While he cannot access their true valuations, he can design a mechanism which maximizes the total value at any bid profile. That is our definition of $\mathcal{M}^s(\mathcal{V})$. Using such a kind of mechanism, the goal is achieved when every bidder bids truthfully.
For a single item, every mechanism in the family $(M_k)_{k:\mathbb{N}^*}$ introduced in Section 3.1 satisfies the condition of $\mathcal{M}^s$ and the only computation required is to find the maximum bid which is a real number. Moreover, in some auction forms like the English or Dutch auctions, the bids are already sorted during collection. The case of multi-item auctions, either identical items or combinatorial, is more complicated in terms of computation. The difficulty arises from the restriction on feasibility of allocations on top of the valuation space's high dimensionality. While such computational problems are already addressed in the field of Algorithmic Mechanism Design (see for example [6]), insights from mathematical properties of the valuation space can be useful as we shall see.
As mentioned in Section 3.2, we assume that the valuation space $\mathcal{V}$ is compact. Therefore, we have a finite cover with open balls of radius γ. If we can define "simple" and optimal mechanisms on each of these open balls, then our problem is reduced to glueing them together to obtain a "simple" and optimal mechanism on $\mathcal{V}$. For instance, if we can define a mechanism on each open ball by taking a constant allocation profile which maximizes the total value at each bid profile, then the remaining task to obtain a mechanism M on $\mathcal{V}$ is to choose the values of M on the intersections of the balls. Proposition 3.3.1 states that the total values from any two valuation profiles which are close to each other by γ have the same maximizers.

Proposition 3.3.1 *Let $v^0 : \mathcal{F}_\gamma$ and $v^1 : B(v^0, \gamma)$. Then,*

$$\arg max\ A \mapsto \Psi(v^0, A) = \arg max\ A \mapsto \Psi(v^1, A).$$

***Proof*:** Let $A^0 : \arg max\ A \mapsto \Psi(v^0, A)$ and $A^1 : \mathcal{A}$. There are two cases to consider.

- First case: $A^1 \notin \arg max\ A \mapsto \Psi(v^0, A)$. It means that

$$\sum_{i:\mathcal{B}} v_i^0(A_i^1) < \sum_{i:\mathcal{B}} v_i^0(A_i^0).$$

From Equation (3.2.1) defining the space $\mathcal{F}_\gamma$, there exists $k : \mathbb{N}^*$ such that

$$\sum_{i:\mathcal{B}} v_i^0(A_i^1) < \sum_{i:\mathcal{B}} v_i^0(A_i^0) - 2bk\gamma. \tag{3.3.1}$$

Besides, since $d(v^0, v^1) < \gamma$, for all $i : \mathcal{B}$ and for all $I : \mathbb{I}$,

$$v_i^0(I) - \gamma < v_i^1(I) < v_i^0(I) + \gamma.$$

It follows that

$$\sum_{i:\mathcal{B}} v_i^0(A_i^0) - b\gamma < \sum_{i:\mathcal{B}} v_i^1(A_i^0) < \sum_{i:\mathcal{B}} v_i^0(A_i^0) + b\gamma, \tag{3.3.2}$$

and

$$\sum_{i:\mathcal{B}} v_i^0(A_i^1) - b\gamma < \sum_{i:\mathcal{B}} v_i^1(A_i^1) < \sum_{i:\mathcal{B}} v_i^0(A_i^1) + b\gamma. \tag{3.3.3}$$

Therefore,

$$\begin{aligned}
&\textstyle\sum_{i:\mathcal{B}} v_i^1(A_i^1) \\
&< && \text{Inequality (3.3.3)} \\
&\textstyle\sum_{i:\mathcal{B}} v_i^0(A_i^1) + b\gamma \\
&< && \text{Inequality (3.3.1)} \\
&\textstyle\sum_{i:\mathcal{B}} v_i^0(A_i^0) - 2bk\gamma + b\gamma \\
&< && k \geq 1 \text{ and Inequality (3.3.2)} \\
&\textstyle\sum_{i:\mathcal{B}} v_i^1(A_i^0).
\end{aligned}$$

- Second case: $A^1 \in \arg max\ A \mapsto \Psi(v^0, A)$. Then,

$$\sum_{i:\mathcal{B}} v_i^0(A_i^1) = \sum_{i:\mathcal{B}} v_i^0(A_i^0).$$

From Inequality (3.3.2) and Inequality (3.3.3), we obtain

$$\left| \sum_{i:\mathcal{B}} v_i^1(A_i^1) - \sum_{i:\mathcal{B}} v_i^1(A_i^0) \right| < 2b\gamma.$$

From Equation (3.2.1),

$$\sum_{i:\mathcal{B}} v_i^1(A_i^1) = \sum_{i:\mathcal{B}} v_i^1(A_i^0).$$

Thus, $A^0 \in \arg max\ A \mapsto \Psi(v^1, A)$ and

$$\arg max\ A \mapsto \Psi(v^0, A) \subseteq \arg max\ A \mapsto \Psi(v^1, A).$$

By symmetry, we also have

$$\arg max\ A \mapsto \Psi(v^1, A) \subseteq \arg max\ A \mapsto \Psi(v^0, A).$$

□

Note that the existence of a minimum gap $2b\gamma$ in the valuations plays an important role in this proof.
From Proposition 3.3.1, if the distance between two balls (minimum distance between their elements) is smaller than γ, then any two valuation profiles v^0 and v^1 in their union also satisfy the equality

$$\arg max\ A \mapsto \Psi(v^0, A) = \arg max\ A \mapsto \Psi(v^1, A).$$

Hence, the set valued function

$$v \mapsto (\arg max\ A \mapsto \Psi(v, A))$$

is constant on every connected component of $\mathcal{V}$. Particularly, it is constant on $\mathcal{V}$ if $\mathcal{V}$ is convex.

3.4 Collective Truthful Bidding

In Section 2.3, we defined the mechanism space $\mathcal{M}^u(\mathcal{V})$ whose elements ensure truthful bidding when the bidder's goal is to maximize only his own utility. With these mechanisms, even if the bidders communicate their strategies to each other, they still have incentive to bid their true valuation profile v as their utilities (which are their respective maximum utilities) are the same as they would get for any other bid profile in

$$\cap_{i:\mathcal{B}} \arg max\ v' \mapsto U_i(v, M(v')).$$

Moreover, Proposition 3.4.1 states that with a mechanism M in $\mathcal{M}^u(\mathcal{V})$, no matter what the valuation profile, when bidder i is allocated the same item, he has to pay the same price.

Proposition 3.4.1 *Let $\mathcal{V} \subseteq \mathcal{F}_\gamma$ and $M : \mathcal{M}^u(\mathcal{V})$. For a bidder $i : \mathcal{B}$ and for every two valuation profiles $v^0, v^1 : \mathcal{V}$,*

$$M(v^0).A_i = M(v^1).A_i \Rightarrow M(v^0).p_i = M(v^1).p_i.$$

***Proof*:** Suppose $M(v^0).A_i = M(v^1).A_i$. Since $M \in \mathcal{M}^u(\mathcal{V})$, we have

$$v^0 \in \arg max\ v' \mapsto U_i(v^0, M(v')),$$

which implies that:

$$v_i^0(M(v^0).A_i) - M(v^0).p_i \geq v_i^0(M(v^1).A_i) - M(v^1).p_i.$$

It follows that $M(v^0).p_i \leq M(v^1).p_i$.
By symmetry, we also have $M(v^1).p_i \leq M(v^0).p_i$.

□

Consequently, if M assigns the same allocation profile to every bid profile in

$$\cap_{i:\mathcal{B}} \arg max\ v' \mapsto U_i(v, M(v')),$$

then every bidder pays the same price to maximize his utility. Hence, the seller earns the same revenue.
Furthermore, Proposition 3.4.2 shows that if a bid profile is close to v with a distance less than γ (the minimum gap as introduced in Section 3.2), then the mechanism M does not have to assign the same allocation profile as does v to this bid profile to yield the same revenue to the seller. If M maximizes the total value and ensures collective truthful bidding at the same time, then the seller's revenue is constant on any open ball $B(v^0, \gamma)$ with $v^0 : \mathcal{V}$.

Proposition 3.4.2 *Let $v^0 : \mathcal{V}$ and $M : \mathcal{M}^s(B(v^0, \gamma)) \cap \mathcal{M}^u(B(v^0, \gamma))$. Then, for all $v^1 : B(v^0, \gamma)$,*

$$\sum_{i:\mathcal{B}} M(v^1).p_i = \sum_{i:\mathcal{B}} M(v^0).p_i.$$

***Proof*:** Let $v^1 : B(v^0, \gamma)$. Since $M \in \mathcal{M}^u(B(v^0, \gamma))$, for all $i : \mathcal{B}$

$$v_i^1(M(v^1).A_i) - M(v^1).p_i \geq v_i^1(M(v^0).A_i) - M(v^0).p_i.$$

By summing over $\mathcal{B}$, we obtain

$$\sum_{i:\mathcal{B}} v_i^1(M(v^1).A_i) - \sum_{i:\mathcal{B}} M(v^1).p_i \geq \sum_{i:\mathcal{B}} v_i^1(M(v^0).A_i) - \sum_{i:\mathcal{B}} M(v^0).p_i.$$

From Proposition 3.3.1, $M \in \mathcal{M}^s(B(v^0, \gamma))$ implies that $M(v^1).A$ and $M(v^0).A$ are in

$$\arg max\ A \mapsto \Psi(v^1, A) = \arg max\ A \mapsto \Psi(v^0, A).$$

Therefore,

$$\sum_{i:\mathcal{B}} v_i^1(M(v^1).A_i) = \sum_{i:\mathcal{B}} v_i^1(M(v^0).A_i),$$

and

$$\sum_{i:\mathcal{B}} M(v^1).p_i \leq \sum_{i:\mathcal{B}} M(v^0).p_i.$$

By symmetry, $\sum_{i:\mathcal{B}} M(v^0).p_i \leq \sum_{i:\mathcal{B}} M(v^1).p_i$.

□

Analogous to the extension of Proposition 3.3.1, the latter proposition also extends to any connected component of $\mathcal{V}$; hence it holds for any two points of $\mathcal{V}$ if $\mathcal{V}$ is convex.

3.5 Nash Equilibrium Mechanisms

An alternative introduced in Section 2.3 is the use of Mechanisms for which the actual valuation profile is a pure Nash Equilibrium point. In some cases, it gives more choices of mechanisms than the one described in Section 3.4. Since all inequalities in the definition of $\mathcal{M}^N(\mathcal{V})$ are also part of those for $\mathcal{M}^u(\mathcal{V})$, we have $\mathcal{M}^u(\mathcal{V}) \subseteq \mathcal{M}^N(\mathcal{V})$ for any convex subset $\mathcal{V} \subseteq \mathcal{F}_\gamma$. This inclusion can be strict. As stated in the following example, the single item Second-Price mechanism M_2 is in the difference of the two sets.

Example 3.5.1 *Let* $\alpha_0, \cdots, \alpha_{b-1} : \mathbb{R}_{>0}$. *Then,*

$$M_2 \notin \mathcal{M}^u(\prod_{i=0}^{b-1}[0, \alpha_i]) \text{ and } M_2 \in \mathcal{M}^N(\prod_{i=0}^{b-1}[0, \alpha_i]).$$

As discussed in Section 2.1, bidding the true valuation is a *best response* for any bidder if every other bidders do the same. To see why M_2 is not in $\mathcal{M}^u(\prod_{i=0}^{b-1}[0, \alpha_i])$, it is enough to consider the valuation profile

$$v : i : \mathcal{B} \mapsto \alpha_i : \mathbb{R}_{>0}.$$

The bid profile

$$v' : i : \mathcal{B} \mapsto \alpha_i - \varepsilon : \mathbb{R}_{>0},$$

where $min\{\alpha_i \mid i : \mathcal{B}\} > \varepsilon > 0$ yields a higher utility to the winner.
An example where the standard mechanism M_1 is in $\mathcal{M}^N(\mathcal{V})$ but not in $\mathcal{M}^u(\mathcal{V})$ with $\mathcal{V}$ being not connected is given below.

Example 3.5.2 *Let* $i : \mathcal{B}$ *and* $\alpha_i, \beta_i : \mathbb{R}_{\geq 0}$ *such that* $\alpha_i < \beta_i$. *Consider*

$$\mathcal{V}_{\alpha_i,\beta_i} := ([0, \alpha_i[^{i-1} \times \{\alpha_i\} \times [0, \alpha_i[^{b-i}) \cup ([\alpha_i, \beta_i[^{i-1} \times \{\beta_i\} \times [\alpha_i, \beta_i[^{b-i}).$$

Then, $M_1 \in \mathcal{M}^N(\mathcal{V}_{\alpha_i,\beta_i})$ *and* $M_1 \notin \mathcal{M}^u(\mathcal{V}_{\alpha_i,\beta_i})$.

In this case, it is a best response for a bidder to bid truthfully if everyone else does the same. However, if bidder i has the value β_i, then he would increase his utility if they all bid lower than α_i.

Since the kind of mechanism in question in this section does not guarantee truthful bidding unless the bidders are independent, the bid collection rules that should accompany them must preserve the independence, which we assume holds initially, while the bidders are allowed to bid.

We saw in Chapter 2 that a bidder i's valuation can change "naturally" from one state to the next in an auction. Following our comment in Section 2.1 concerning its origin (being a realization of a certain random variable), we now can think of the sequence of changes in v_i as a path of a certain stochastic process. Given a set of available bids at a time t, i chooses his bid according to his valuation at that time and to what he knows about his opponents. Hence if we think of his bid at time $t+1$ as given by a random variable, then we can say that it depends on the random variable giving his valuation at time t. As for its relation to the other bidders' valuations (at t) or bids (at $t+1$), assumptions on independence are needed. At least, we should assume something about the random variables giving the the bidders' valuations. For instance in the literature, there are the *Independent Value Model*, the *Common Value Model* and the *Affiliated Value Model* as surveyed in [17]. Our approach using the sets $\mathcal{V}_{a,i}$'s avoids such assumptions.

Although we consider fixed sets of available bids, we do not eliminate the "dependence on chance" [22]. Recall that in Section 2.3, we informally defined the statement "i and j are independent" by "none of them is certain about the other's valuation nor bid". When each bidder has more than two available strategies (may be infinite), we assume that they can freely choose any. In that case, no bidder has control of the other's bid and we have "mutual independence" when no bidder *knows* the other's valuation. In John Nash's terminology as in [23], we can say that each bidder thinks of his opponent's strategy as *mixed* (a convex combination of his available strategies).

If bidder j has a single available strategy, then "i is independent of j" should mean that i does not *know* j's strategy nor his valuation. Following Section 2.5, we define *independence* as follows. We say that i is *independent* of j in state $s : \mathit{State}[\mathcal{V}]$ and we write $i\mathcal{I}(s)j$ if and only if

$$i\mathcal{I}(s)j : \neg\, K_i(s.v_j) \wedge (K_i(s.\mathcal{V}_{a,j}) \Rightarrow \#s.\mathcal{V}_{a,j} > 1)\,.$$

By the definition of K_i given in Section 2.5, each bidder knows his own valuation and available bids. Hence the relation $\mathcal{I}(s)$ is irreflexive for every state $s : \mathit{State}[\mathcal{V}]$.

Moreover, if i is uncertain about j and j about k, it does not necessarily mean that i is uncertain about k. Especially, i is not independent of himself whether or not there exists another bidder j with whom he is mutually independent. Assuming that all bidders are independent of each other at a state $s : \mathit{State}[\mathcal{V}]$, we have $\mathcal{I}(s)$ symmetric. It follows that $\mathcal{I}(s)$ is not transitive.

3.6 Chapter Summary

In this chapter, we have explored the properties of valuation spaces to obtain insights for the mechanism spaces. We have seen that if the valuation space is convex and compact in $(\mathcal{F}_\gamma, d)$, then the set of allocation profiles that maximize the total value is the same for every profile in that space. It means that once such a space is defined, any additional optimization can be done over that common set of allocation profiles.

We have proved that if the mechanism defined on a compact convex valuation space ensures collective truthful bidding, then the price it assigns for a particular allocation is fixed regardless of the valuation profile. If in addition its allocation profiles maximize the total value, then the seller's revenue is constant on the valuation space. These characterizations show the availability of truthful mechanisms that are relatively simple.

Finally, we have discussed a mechanism space which uses the concept of Nash Equilibria. We have defined a notion of *independence* which is required in using such mechanism. For this, we have assumed that a bidder is free to chose any of his many available bids (when it is the case). It prevents a bidder from being sure that another bidder he colludes with would not break their agreement if the latter has two or more available bids. In Chapter 4, we will discuss independence in sealed-bid auctions.

Chapter 4

Distributed Sealed-Bid Auctions

The success of auction platforms like eBay using combinations of open and sealed-bid auctions is well-known. While such a combination is promoted [24], in this chapter we focus on distributing sealed-bid auctions. We consider the auctioneer/seller as a special kind of bidder who bids his reserve price.
In Sections 4.1 and 4.2, we describe how the bids are communicated and how the results are computed. In Section 4.3, we formalize the rules guiding these operations while in Sections 4.4 and 4.5, we discuss the consequences of these rules from a bidder's perspective.

4.1 Messages in Sealed-Bid Auctions

Translating the rules of a sealed-bid auction room, the bids in distributed sealed-bid auctions should be submitted in some "sealed" form and "opened" only when the bidding is over. Following Section 2.4, there is no auctioneer who keeps the "envelops" and opens them at the end. Instead, every bidder *commits* his bid during the bidding time which ends according to the participant's cooperative decision, then *reveals* it when the bidding time is over.
In Section 2.4, we described a type *OMES* of messages containing the bidder's identity $id : \mathcal{B}$ and his bid $oBid : \mathcal{F}$ which are used here to reveal a bid. For committing it, we consider another type *SMES* of messages which play the role of sealed envelops. Such a message contains an encrypted value of the bid it represents, the one-way function used to encrypt the bid and the identity of the bidder.
As we shall see in the example of Chapter 5, the set of all possible bid can be relatively small. In that case, access to the one-way function would give a bidder access to the others' actual bids. To encounter this problem, we can replace the one-way function in the *SMES* message by its own encryption. Alternatively, we can extend the set of bids in a way that it is large enough and every element in the difference is related to a unique possible bid in the original set.

Denote by $\mathcal{E}$ the space of encrypted bids and by $\mathcal{G}$ the space of one-way functions from $\mathcal{F}$ to $\mathcal{E}$. Then, the type *SMES* is described as in the left schema.

SMES

$id : \mathcal{B}$
$sBid : \mathcal{E}$
$seal : \mathcal{G}$

OMES

$id : \mathcal{B}$
$oBid : \mathcal{F}$
$sBid : \mathcal{E}$

In this description of *OMES*, we added the encrypted bid *sBid* to link the "opened envelop" with the "sealed" one. When a bidder prepares a bid, he writes two messages: $sm : SMES$ and $om : OMES$ to commit and reveal the bid respectively. Therefore, both messages contain his identity and the encrypted bid $sm.sBid$ which he obtained by computing $sm.seal(om.oBid)$. When they are ready, these two messages are put in a single record (of type *UREC*).

UREC

$sm : SMES$
$om : OMES$

$sm.id = om.id$
$sm.sBid = om.sBid = sm.seal(om.oBid)$

Being allowed to change his bid during the appropriate time, each bidder i has a sequence $uRec_i : \operatorname{seq} UREC$ recording the corresponding pairs of messages to all his previous bids.

4.2 Operations in Sealed-Bid Auctions

When a bidder i executes any operation (committing or revealing a bid, reading a sealed or opened bid, computing the result or transacting), the name of that operation is noted in a sequence $fHist_i : \operatorname{seq} STRING$. It is important to emphasize that $fHist_i$ is not intended to record the history of the auction (which is the purpose of aS) but to monitor the use of these operations in order to locally separate the three phases of the auction: *committing*, *revealing* and *computing*.
The bids are committed by broadcasting their sealed forms. Each bidder i records the sealed bid messages he receives or sends in a set $sRec_i : \mathbb{P}\, SMES$. The two following schemas summarize the operations *SealBid* and *SRead* which

i uses to send and receive these messages respectively.

SealBid

$\Delta SBState[\mathcal{V}]$
$m! : SMES$
$rec : UREC$

$rec.sm = m! \land m!.id = i$
$sRec_i' = sRec_i \cup \{m!\}$
$uRec_i' = uRec_i \frown \langle rec \rangle$
$fHist_i' = fHist_i \frown \langle \text{“}SealBid\text{”} \rangle$

SRead

$\Delta SBState[\mathcal{V}]$
$mSet? : \mathbb{P}\, SMES$

$sRec_i' = sRec_i \cup mSet?$
$fHist_i' = fHist_i \frown \langle \text{“}SRead\text{”} \rangle$

Similarly and as introduced in Section 2.4, each bidder records the open bid messages he receives or sends in a set $oRec_i : OMES$ during the revealing phase. The operations for this phase are described below.

OpenBid

$\Delta SBState[\mathcal{V}]$
$m! : OMES$

$m! = last(uRec_i).om$
$oRec_i' = oRec \cup \{m!\}$
$fHist_i' = fHist_i \frown \langle \text{“}OpenBid\text{”} \rangle$

ORead

$\Delta SBState[\mathcal{V}]$
$mSet? : \mathbb{P}\, OMES$

$oRec_i' = oRec_i \cup mSet?$
$fHist_i' = fHist_i \frown \langle \text{“}ORead\text{”} \rangle$

Note from the *OpenBid* operation's description that only the last bid is revealed for every bidder. All preconditions for these operations as well as for those which follow are given in Section 4.3 as they are part of the collection rules.

Assuming that the broadcasts succeed and that there is at most one open bid per bidder, every participant acquires the same bid profile $v : \mathcal{B} \to \mathcal{F}$ at the end of the revealing phase. If some bidders did not reveal their bids, each missing valuation is set to be the constant function equal to zero which is simply denoted by $\lambda\, I : \mathbb{I} \bullet 0$. Since the bidders also have the auction mechanism M, assuming that they all have the computational power, each of them can compute the result and update the observable $res_i : OUTCOME$.

Results

$\Delta SBState[\mathcal{V}]$
$v : \mathcal{B} \to \mathcal{F}$

$\forall\, m : oRec_i \bullet v(m.id) = m.oBid$
$\forall\, i : \mathcal{B} \setminus \{m.id \mid m \in oRec_i\} \bullet v(i) = \lambda\, I : \mathbb{I} \bullet 0$
$res_i' = M(v)$
$fHist_i' = fHist_i \frown \langle \text{“}Results\text{”} \rangle$

The seller, considered as a special bidder, particularly has the result under these assumptions. The transaction as well as the registration process are outside the scope of the present document.

4.3 Sealed-Bid Collection Rules

Following the previous description of the sealed-bid auctions, we see that the set $\{R_k \mid k \in [0,4]\}$ is a proper subset of the set $\mathcal{R}_S$ of their collection rules. Before we give the extra rules, let us modify the definition of auction global states to include information about the sealed bid messages as well as the performed operations and the result.
In addition to the local observables described in Sections 4.1 and 4.2 and to the observables introduced in Chapter 2, we define a set $asRec : \mathbb{P}\, SMES$ of sealed bid messages that are broadcast in the system. In other words, $asRec$ is to the committing phase the same as $aoRec$ is to the revealing phase. The global state of a sealed-bid auction is summarized in the following schema.

$SBState[\mathcal{V}]$

$$
\begin{array}{l}
v : \mathcal{B} \to \mathcal{F} \\
\mathcal{V}_a : \mathcal{B} \to \mathbb{P}\, \mathcal{F} \\
sRec : \mathcal{B} \to \mathbb{P}\, SMES \\
oRec : \mathcal{B} \to \mathbb{P}\, OMES \\
uRec : \mathcal{B} \to \text{seq}\, UREC \\
res : \mathcal{B} \to OUTCOME \\
fHist : \mathcal{B} \to \text{seq}\, STRING \\
asRec : \mathbb{P}\, SMES \\
aoRec : \mathbb{P}\, OMES \\
\hline
\forall\, i : \mathcal{B} \bullet v_i \in \mathcal{V}_{a,i} \land \mathcal{V}_{a,i} \subseteq \mathcal{V}_i \\
\forall\, i : \mathcal{B}, \forall\, k : \text{dom}\, uRec_i \bullet uRec_i[k].sm \in oRec_i
\end{array}
$$

Note that while in the general definition of $State[\mathcal{V}]$, the valuation v_i of bidder i is required only to be in the projection $\mathcal{V}_i$ of the valuation space, for $SBState[\mathcal{V}]$, it is necessarily an available bid. Also note from the second line in the invariants of $SBState[\mathcal{V}]$ that the only way to add a record $rec : UREC$ to $uRec_i$ is through the operation $SealBid$.
Analogous to the rules in $\{R_k \mid k \in [0,3]\}$ which concern open bid messages, we have the four first proper rules of sealed-bid auctions.
Firstly, the set of broadcast sealed bid messages is initially empty.

$$R_{S,0}(aS) := aS[0].asRec = \{\}.$$

Secondly, a sealed bid message received by any bidder i must have been broadcast.

$$R_{S,1}(aS) := \forall\, t : \mathbb{N}, \forall\, i : \mathcal{B} \bullet aS[t].sRec_i \subseteq aS[t].asRec.$$

As R_0 and R_1 imply that $aS[0].oRec_i$ is empty, $R_{S,0}$ and $R_{S,1}$ also imply that $aS[0].sRec_i$ is. Thirdly, since sending and receiving cannot be undone, a sent

or received sealed bid message remains in this status throughout the rest of the auction.

$$R_{S,2}(aS) := \forall\, t^0, t^1 : \mathbb{N} \bullet (t^0 < t^1) \Rightarrow (aS[t^0].asRec \subseteq aS[t^1].asRec)$$
$$R_{S,3}(aS) := \forall\, t^0, t^1 : \mathbb{N}, \forall\, i : \mathcal{B} \bullet (t^0 < t^1) \Rightarrow (aS[t^0].sRec_i \subseteq aS[t^1].sRec_i).$$

Apart from R_0 and $R_{S,0}$, we have two more initialization rule. The observable $res_i : OUTCOME$ that changes after running the *Results* operation is initially set to be the outcome which has a constant allocation profile equal to $\perp$ and a constant price profile equal to 0. Denote it by $(\perp, 0)$.

$$R_{S,4}(aS) := \forall\, i : \mathcal{B} \bullet aS[0].res_i = (\perp, 0).$$

For the sequences $uRec_i$ and $fHist_i$, we set them initially empty by the following rule:

$$R_{S,5}(aS) := \forall\, i : \mathcal{B} \bullet aS[0].uRec_i = \langle\,\rangle \wedge aS[0].fHist_i = \langle\,\rangle.$$

As described in Section 4.2, the sequence $fHist_i$ of operation names follows some rules to locally separate the phases. First, a bidder can never read any open bid message before committing his own bid. This rule notes the key feature of sealed-bid auction games.

$$R_{S,6}(aS) := \forall\, t : \mathbb{N}, \forall\, i : \mathcal{B}, \forall\, k, l \in \mathrm{dom}(aS[t].fHist_i) \bullet$$
$$(aS[t].fHist_i[k] = \text{“}SealBid\text{”} \wedge l \leq k) \Rightarrow aS[t].fHist_i[l] \neq \text{“}ORead\text{”}.$$

The next rule says that once a bidder reveals his last bid, he no longer can commit a different bid:

$$R_{S,7}(aS) := \forall\, t : \mathbb{N}, \forall\, i : \mathcal{B}, \forall\, k, l \in \mathrm{dom}(aS[t].fHist_i) \bullet$$
$$(aS[t].fHist_i[k] = \text{“}SealBid\text{”} \wedge l \leq k) \Rightarrow aS[t].fHist_i[l] \neq \text{“}OpenBid\text{”}.$$

Note that this rule ensures that the valuation profile the bidders obtain at the end of the sealed-bid auction is well defined.
With the two last rules, if a bidder does not read or send any open bid message, then he can still commit a bid. Therefore, if by any means he accesses the other's open bid, then he gains the privilege to bid properly. To ensure that no bidder has an incentive to seek for an outside source, we impose a rule saying that after a bidder has read an open bid message, he no longer reads any sealed bid message:

$$R_{S,8}(aS) := \forall\, t : \mathbb{N}, \forall\, i : \mathcal{B}, \forall\, k, l \in \mathrm{dom}(aS[t].fHist_i) \bullet$$
$$(aS[t].fHist_i[k] = \text{“}SRead\text{”} \wedge l \leq k) \Rightarrow aS[t].fHist_i[l] \neq \text{“}ORead\text{”}.$$

In addition, a bidder cannot perform any of the bidding operations after computing the result:

$$R_{S,9}(aS) := \forall\, t : \mathbb{N}, \forall\, i : \mathcal{B}, \forall\, k, l \in \mathrm{dom}(aS[t].fHist_i) \bullet \\ (aS[t].fHist_i[k] = \text{“}SRead\text{”} \land l > k) \Rightarrow \\ aS[t].fHist_i[l] \notin \{\text{“}SealBid\text{”}, \text{“}SRead\text{”}, \text{“}OpenBid\text{”}, \text{“}ORead\text{”}\}.$$

Note that we could write the rules for separating the bidding phases using $asRec$ and $aoRec$. But as they are not clear from the operations, it is convenient to use $fHist_i$.
Now, we have $\mathcal{R}_S = \{R_k \mid k \in [0,4]\} \cup \{R_{S,k} \mid k \in [0,9]\}$.
Following $R_{S,6}$, $R_{S,7}$ and $R_{S,9}$, since the operation $SealBid$ appends the string “$SealBid$” to $fHist_i$, the strings “$ORead$”, “$OpenBid$” and “$Results$” must not be in the range of $fHist_i$ as a precondition for $SealBid$. Since adding elements to $uRec_i$ or $sRec_i$ has no condition, there is no other precondition for $SealBid$:

pre $SealBid$

$SBState[\mathcal{V}]$

“$ORead$”, “$OpenBid$”, “$Results$” $\notin \mathrm{ran}(fHist_i)$

Similarly, since “$SRead$” is added to $fHist_i$ during $SRead$, the rules $R_{S,8}$ and $R_{S,9}$ implies that the strings “$ORead$” and “$Results$” must not be in the range of $fHist_i$ to run the operation. As the change for $sRec_i$ in the operation is the addition of some elements, we only have the previous precondition:

pre $SRead$

$SBState[\mathcal{V}]$

“$ORead$”, “$Results$” $\notin \mathrm{ran}(fHist_i)$

Note that it is possible that “$OpenBid$” $\in \mathrm{ran}(fHist_i)$.
The rule $R_{S,9}$ also implies that $\mathrm{ran}(fHist_i)$ must not contain “$Results$” before running $ORead$:

pre $ORead$

$SBState[\mathcal{V}]$

“$Results$” $\notin \mathrm{ran}(fHist)$

For the $OpenBid$ operation, since the message to send should come from the sequence $uRec_i$, this sequence must be non-empty as a precondition for $OpenBid$. Therefore, we also have “$SealBid$” $\in \mathrm{ran}(fHist_i)$. As for the other bidding operations, $R_{S,9}$ implies that the string “$Results$” should not be in $\mathrm{ran}(fHist_i)$:

pre *OpenBid*

$SBState[\mathcal{V}]$

"*Results*" $\notin \mathrm{ran}(fHist_i)$

$uRec_i \neq \langle\,\rangle$

Although $R_{S,6}$ to $R_{S,9}$ are defined to separate the phases, they do not imply that each of these three phases exists locally. Furthermore, they do not allow us to infer the existence of an earlier phase given a later one. Particularly, since the *Results* operation does not require $oRec_i$ or $fHist_i$ to be non-empty, it can be performed without any preceding bidding phase according to the rules.

4.4 A Bidder's View of the System

As we added more observables to the local states, we now need to discuss the definitions of the equivalence relations $\sim_i$ given in Section 2.5. Keeping the meaning of these relations the same, we say that two global states $s^0, s^1 : SBState[\mathcal{V}]$ are equivalent for bidder i if his local states in s^0 and s^1 are the same. Specifically, we write $s^0 \sim'_i s^1$ if and only if

$$s^0.sRec_i = s^1.sRec_i \wedge s^0.oRec_i = s^1.oRec_i \wedge s^0.uRec_i = s^1.uRec_i \\ \wedge\, s^0.fHist_i = s^1.fHist_i \wedge s^0.v_i = s^1.v_i \wedge s^0.\mathcal{V}_{a,i} = s^1.\mathcal{V}_{a,i}.$$

Note that the equalities $s^0.oRec_i = s^1.oRec_i$ and $s^0.fHist_i = s^1.fHist_i$ imply that $s^0.res_i = s^1.res_i$ as the string "*Results*" must be either the last element of $s^0.fHist_i$ or not in its range at all.
Since $\sim'_i$ are again equivalence relations, we have all the concepts and properties introduced in Section 2.5. Given the mechanism M of a sealed-bid auction, we consider the structure $\mathcal{K}'(M, \mathcal{R}_S)$.
In Section 2.4 while defining R_4, we said that when an open bid message is broadcast, we qualify the bid as *valid*. But before it can be broadcast, R_4 states that the bid must be available to the bidder. Moreover, the definition of *OpenBid* implies that any bidder i's open bid is recorded in the sequence $uRec_i$. Since the recording of the pairs of bid messages is done in the operation *SealBid*, any valid open bid must have been committed. Defining the proposition

$$P^3(s) := \forall\, om : s.aoRec \bullet \exists\, sm : s.asRec \bullet \\ sm.id = om.id \wedge sm.sBid = om.sBid = sm.seal(om.oBid),$$

we have

$$(\mathcal{K}'(M, \mathcal{R}_S), auc, t) \vDash P^3$$

for all $(auc, t) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$. If we are to allow message delay, the local sets $sRec_i$ and $oRec_i$ might not have similar property as P^3. However, following R_1, if a bidder receives an open bid message $om : OMES$ at (auc, t), then this open bid must have been committed. Writing

$$P^4(s) := \forall\, om : s.oRec_i \bullet \exists\, sm : s.asRec \bullet \\ sm.id = om.id \wedge sm.sBid = om.sBid = sm.seal(om.oBid),$$

we also have

$$(\mathcal{K}'(M, \mathcal{R}_S), auc, t) \vDash (\forall\, i : \mathcal{B}, P^4)$$

at any point $(auc, t) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$. From the Knowledge Generalization Rule, we see that each bidder i knows that any open bid he receives has been committed:

$$\forall (auc, t) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}, \forall\, i : \mathcal{B} \bullet (\mathcal{K}'(M, \mathcal{R}_S), auc, t) \vDash K_i P^4.$$

Note that this result does not depend on the equations in the definition of $\sim_i'$. Since $sRec_i$ contains sealed bid messages whose contents do not serve i in his decision on a new bid as $fHist_i$ and $uRec_i$ do not, we can remove the equations concerning these observables and get the equivalence relation $\sim_i$ back. Recall that $s^0 \sim_i s^1$ if and only if

$$s^0.oRec_i = s^1.oRec_i \wedge s^0.v_i = s^1.v_i \wedge s^0.\mathcal{V}_{a,i} = s^1.\mathcal{V}_{a,i}.$$

To summarize, we have the following proposition.

Proposition 4.4.1 *Consider the equivalence relation $\sim_i$ for all $i : \mathcal{B}$ and let $\mathcal{K}(M, \mathcal{R}_S)$ be the corresponding structure. Then,*

$$(\mathcal{K}(M, \mathcal{R}_S), auc, t) \vDash K_i P^4$$

for all point $(auc, t) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$ and for any bidder $i : \mathcal{B}$.

4.5 Independence between Bidders

As mentioned in Section 3.5, some important mechanisms (including the single item standard ones like M_1 and M_2) need to be used with bid collection rules that preserve independence while the bidders are allowed to bid. Referring to the previous sections, this means that independence should hold until the bidders no longer can seal a bid for the sealed-bid auction form to be compatible with these mechanisms. Let M be such mechanism.
Assume that the bidders are mutually independent at the beginning of a sealed-bid auction $auc : AUC[(M, \mathcal{R}_S)]$. Formally, assume that

$$(\mathcal{K}(M, \mathcal{R}_S), auc, 0) \vDash (\forall\, i, j : \mathcal{B} \bullet (i = j) \vee i \mathcal{I} j).$$

Each bidder $i : \mathcal{B}$ does not know the exact valuation of any other bidder $j : \mathcal{B} \setminus \{i\}$ nor his single available bid if it is the case. By definitions (D_3) and (D_2), the first part concerning j's valuation means that there exists a point $(auc^{i,j,0}, t^{i,j,0}) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$ such that

- $(auc^{i,j,0}, t^{i,j,0}) \sim_i (auc, 0)$ and
- $auc^{i,j,0}.aS[t^{i,j,0}].v_j \neq auc.aS[0].v_j$.

The second part means that if for every point $(auc^{i,j,1}, t^{i,j,1}) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$ equivalent to $(auc, 0)$ with respect to $\sim_i$

$$auc^{i,j,1}.aS[t^{i,j,1}].\mathcal{V}_{a,j} = auc.aS[0].\mathcal{V}_{a,j},$$

then $\#auc.aS[0].\mathcal{V}_{a,j} > 1$.
Let $t : \mathbb{N}$ be a time when bidder i can still seal a bid in the next step. Then, from the precondition of *SealBid*,

$$\text{“}ORead\text{”}, \text{“}OpenBid\text{”}, \text{“}Results\text{”} \notin \mathrm{ran}(auc.aS[t].fHist_i).$$

Therefore,

$$\begin{aligned} auc.aS[t].oRec_i &= auc.aS[0].oRec_i \\ &= auc^{i,j,1}.aS[t^{i,j,1}].oRec_i \end{aligned}$$

for any point $(auc^{i,j,1}, t^{i,j,1}) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$ equivalent to $(auc, 0)$ with respect to $\sim_i$.
As mentioned before, no operation in a sealed-bid auction changes i's valuation or set of available bids but they might change “naturally”. Since they are the same in $auc.aS[0]$ and $auc^{i,j,1}.aS[t^{i,j,1}]$ for any point $(auc^{i,j,1}, t^{i,j,1}) \sim_i (auc, 0)$, these external changes can occur in any of these states. Hence we can construct a point in $AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$ from any $(auc^{i,j,1}, t^{i,j,1}) \sim_i (auc, 0)$ in a way that preserves every observables apart from v_i and $\mathcal{V}_{a,i}$ which are set equal to $auc.aS[t].v_i$ and $auc.aS[t].\mathcal{V}_{a,i}$ respectively.
If $auc.aS[t].v_j = auc.aS[0].v_j$, then we construct a point $(auc^{i,j,2}, t^{i,j,2})$ equivalent to (auc, t) with respect to $\sim_i$ and satisfying the condition

$$auc^{i,j,2}.aS[t^{i,j,2}].v_j \neq auc.aS[t].v_j$$

from $(auc^{i,j,0}, t^{i,j,0})$. If $auc.aS[t].v_j \neq auc.aS[0].v_j$, then we construct such a point from $(auc, 0)$ itself as $\sim_i$ is reflexive. Hence, we have the following lemma.

Lemma 4.5.1 *Let* $(auc, t) : AUC[M, \mathcal{R}_S] \times \mathbb{N}$ *and* $i, j : \mathcal{B}$. *Then*

$$(\mathcal{K}(M, \mathcal{R}_S), auc, 0) \vDash \neg\, K_i(v_j)$$

implies that

$$(\mathcal{K}(M, \mathcal{R}_S), auc, t) \vDash \neg\, K_i(v_j) \mathbf{U} \neg\ pre\, SealBid_i.$$

(The index i in $SealBid_i$ means that the operation is to be run by bidder i). As above, assume that $\#auc.aS[t].\mathcal{V}_{a,j} = 1$. If $auc.aS[t].\mathcal{V}_{a,j} = auc.aS[0].\mathcal{V}_{a,j}$, then there exists $(auc^{i,j,1}, t^{i,j,1}) : AUC[(M, \mathcal{R}_S)] \times \mathbb{N}$ equivalent to $(auc, 0)$ with respect to $\sim_i$ such that

$$auc^{i,j,1}.aS[t^{i,j,1}].\mathcal{V}_{a,j} \neq auc.aS[0].\mathcal{V}_{a,j}.$$

We can construct a point $(auc^{i,j,2}, t^{i,j,2})$ equivalent to (auc, t) with respect to $\sim_i$ and satisfying

$$auc^{i,j,2}.aS[t^{i,j,2}].\mathcal{V}_{a,j} \neq auc.aS[t].\mathcal{V}_{a,j}$$

from $(auc^{i,j,1}, t^{i,j,1})$. If $auc.aS[t].\mathcal{V}_{a,j} \neq auc.aS[0].\mathcal{V}_{a,j}$, then we construct such a point from $(auc, 0)$ (again following reflexivity of $\sim_i$). Therefore, we also have the subsequent lemma.

Lemma 4.5.2 *Let* $(auc, t) : AUC[M, \mathcal{R}_S] \times \mathbb{N}$ *and* $i, j : \mathcal{B}$. *Then*

$$(\mathcal{K}(M, \mathcal{R}_S), auc, 0) \vDash (K_i(\mathcal{V}_{a,j}) \Rightarrow \#\mathcal{V}_{a,j} > 1)$$

implies that

$$(\mathcal{K}(M, \mathcal{R}_S), auc, t) \vDash (K_i(\mathcal{V}_{a,j}) \Rightarrow \#\mathcal{V}_{a,j} > 1)\mathbf{U}\neg\ pre\, SealBid_i.$$

Combining Lemma 4.5.1 and Lemma 4.5.2, we can infer that a sealed-bid auction $auc : AUC[(M, \mathcal{R}_S)]$ preserves independence during the committing time.

Proposition 4.5.3 *Let* $(auc, t) : AUC[M, \mathcal{R}_S] \times \mathbb{N}$ *and* $i, j : \mathcal{B}$. *Then,*

$$(\mathcal{K}(M, \mathcal{R}_S), auc, 0) \vDash i\mathcal{I}j$$

implies that

$$(\mathcal{K}(M, \mathcal{R}_S), auc, t) \vDash i\mathcal{I}j\mathbf{U}\neg\ pre\, SealBid_i.$$

4.6 Chapter Summary

In this chapter, we have presented a way to distribute sealed-bid auctions. Our approach eliminates the need for some trusted entities to compute the outcome, provided that each bidder has the computational power to do so and that broadcasts are successful. As discussed in Section 3.6, the mechanism can be chosen to be relatively simple depending on the purpose of the auction. Assuming that the system is synchronous and that each phase consists of one round, the protocol needs 3 rounds to collect the bids and to compute the outcome. To make one bid in that case, a bidder needs to send $2b$ messages. We have established that our set of bid collection rules for these auctions preserves independence of the bidders during bidding time. Hence, it is compatible with the mechanisms we discussed in Section 3.5. Particularly, it is compatible with the single item mechanism M_2 which gives the distributed SBSP auctions.

Chapter 5

Application to Tie Breaking

Assuming no ties for our examples so far has allowed us to focus on the rules of auction games. However, as ties might occur, we need to provide a viable solution to break them in the auction game's setting. The protocol we present in this chapter generalizes coin-tossing through an application of distributed sealed-bid auctions. This way, we stay in the setting of auction games.
Besides, as there is no centralized processor to start it, the protocol in question here is a solution to the *Leader Election Problem* [10] on its own.
In Section 5.1, we exploit distributed sealed-bid auctions to produce a protocol for tie breaking and in the remaining sections, we analyse its efficiency.

5.1 Valuation Space and Mechanism

To elucidate the protocol, let us consider the case of two players.
As mentioned above, we do not have a centralized processor to start the protocol. Hence, we need to treat the two players equally. We must choose a sequence of actions that they both perform on their respective sides and a symmetric way of determining the winner. For instance, we may let them both flip a coin (choose 0 or 1 at random) and communicate the results to each other. The issue is that we cannot use deterministic functions like *max* or *min* to decide who wins, otherwise the players would have an incentive to not choose randomly.
The hint is Blum's protocol for *Coin-Flipping by Telephone* as presented in [9]. It consists of letting player i flip a "coin" and commit the result to j who then "guesses" what it was before i reveals it. Bidder j wins if and only if j "guesses" correctly. Although in Blum's protocol, the players' roles are assumed to be established (which exactly is our problem), we can adapt this idea of "guessing" the other's coin into our symmetric setting.
Instead of tossing a coin once, each player does so twice: once for his "fate" and the other as his "guess". If one player guessed correctly and the other did not, then the latter loses. Conversely, if a player loses, then the other player

correctly guessed his first number. Of course it is possible that none or both has/have the right guess but a simple tree of conditional probabilities would show us that we have a winner with probability 0.5.
Generally, assume we have a set W of winners and let $w := \#W \geq 2$. Every player $i \in W$ independently chooses a first number $X_i : [0, w)$ for his "fate" and a second number $Y_i \in [0, w)$ as his "guess". Assume he chooses each of these with equiprobability.
During the appropriate time, each player i commits then reveals the two numbers X_i and Y_i to the others. In terms of auctions, let us say that the bidders (players in W) bid for two items I and J in the sealed-bid form. Bidder i's values for I and J are then respectively X_i and Y_i which he obtained from random variables following a uniform distribution on $[0, w)$ (just as discussed in Section 2.2).
As described in Section 4.1, sealing the bids involves use of a one-way function from the set $\mathcal{F}$ of valuations to a certain space $\mathcal{E}$. However, as the bidders obtain these functions from the same messages containing the sealed bid, trying w^2 possible valuations would not take long for small $w : \mathbb{N}$. Therefore, we consider

$$\mathcal{F} := \{I, J\} \to [0, w)$$

with $[0, w)$ an interval of $\mathbb{R}_{\geq 0}$ (in practice, floating-point numbers) instead of $\mathbb{N}$. With a valuation profile

$$\begin{aligned} v : W &\to \mathcal{F} \\ i &\mapsto v_i, \end{aligned}$$

we have $X_i = \lfloor v_i(I) \rfloor$ and $Y_i = \lfloor v_i(J) \rfloor$ for all $i : W$.
Recall that the mechanism of an auction is a function used to compute the result. It is defined on the valuation space $\mathcal{V}$ and its values in $OUTCOME$ are composed by a feasible allocation profile in $\mathcal{A}$ and a price profile in $W \to \mathbb{R}_{\geq 0}$. Here, we assume the price profile to be the constant function $\lambda\, i : W \bullet 0$.
In Section 2.2, we referred to the choices for which the bidders bid as "items" and we mentioned that they do not need to be physical. Also, we did not give an explicit condition for $\mathcal{A}$ and required it only to be a subset of $W \to \mathbb{I}_\perp$. Therefore, we may allow ourselves to think of I and J to mean "In" and "Out" respectively. A bidder i's value for "In"(X_i) makes him stay "In" the winning position if none of his opponents has the same value for "Out" $(Y_j, j \neq i)$. Writing $I = 1$ and $J = 0$, an allocation profile $A : \mathcal{A}$ is a function on W which takes its values in $\mathbb{B}$ determining whether or not the corresponding player wins. Therefore, we have a mechanism $M^T : \mathcal{V} \to OUTCOME$ such that for all $v : \mathcal{V}$, $M^T(v).p = 0$ and

$$\begin{aligned} M^T(v).A : \ W &\to \mathbb{B} \\ i &\mapsto (\lfloor v_i(1) \rfloor \notin \{\lfloor v_j(0) \rfloor \mid j \neq i\}). \end{aligned}$$

Together with the rules $\mathcal{R}_S$, we have a sealed-bid auction form $AUC[(M^T, \mathcal{R}_S)]$.

5.2 Sequence of Sealed-Bid Auctions

From its definition, the allocation profile in the mechanism M^T may yield any number of players (might be none or all) remaining in their winning positions. If the goal is to obtain a certain number $a : \mathbb{N}$ of winners with $1 \leq a < w$, then we need to run another tie breaking in case $\#(M^T(v).A)^{-1}(\{1\}) \neq a$. There are two cases.

- Firstly, if $\#(M^T(v).A)^{-1}(\{1\}) < a$ then the $w - \#(M^T(v).A)^{-1}(\{1\})$ losers play again to fill the $a - \#(M^T(v).A)^{-1}(\{1\})$ remaining places.
- Secondly, if $\#(M^T(v).A)^{-1}(\{1\}) > a$ then these $\#(M^T(v).A)^{-1}(\{1\})$ winners play for the a winning positions.

In short, we might need a sequence of sealed-bid auctions with different numbers of players and different numbers of prizes to totally break ties.
Representing the state of a tie by the numbers $w : \mathbb{N}$ and $a : \mathbb{N}$ of players and available prizes respectively, a should always be strictly smaller than w unless they are both zero which now means no tie at all.

TState

$w : \mathbb{N}$
$a : \mathbb{N}$

$(0 < a \land a < w) \lor (w = 0 \land a = 0)$

Therefore, each sealed-bid auction in the aforementioned sequence consists of a given state $s : TState$ with $s.a > 0$ and $s.w > s.a$ and some state $s' : TState$ such that $s'.a \in (0, s.a]$ and $s'.w \in (s'.a, s.w]$ or $s' = \mathbf{0}$ where $\mathbf{0}$ is the special state meaning no tie. Note that what completely determines the state s' is the valuation profile v formed in the auction as explained in Section 4.2. Moreover, as mentioned in Section 5.1, each component of the valuation profile in such an auction is assumed to be uniformly chosen from $[0, s.w)$.
We can think of these particular sealed-bid auctions as points in the graph of a function τ mapping a state $s : TState$ to a *distribution* over $TState$ ([25], although in this paper the state space is assumed to be finite). Denote by $\overline{TState}$ the set of distributions over $TState$.
Note that $\tau(\mathbf{0})(\mathbf{0}) = 1$ which means that for any state $s' : TState \setminus \{\mathbf{0}\}$, $\tau(\mathbf{0})(s') = 0$.
Given a state $s : TState \setminus \{\mathbf{0}\}$, we compute $\tau(s)$ in the following. For simplicity, we write w and a for $s.w$ and $s.a$ respectively when the context is clear.

5.3 Probability for $\#(M^T(v).A)^{-1}(\{1\})$

Consider the auction form $AUC[(M^T, \mathcal{R}_S)]$ designed for w bidders who choose their bids for the items I and J with equiprobability. Let

$$\begin{aligned} f : \mathcal{V} &\to [0, w] \\ v &\mapsto f(v) = \#(M^T(v).A)^{-1}(\{1\}). \end{aligned}$$

Following Section 5.2, the state s' as a result of an auction $auc : AUC[(M^T, \mathcal{R}_S)]$ is determined by the valuation profile v in that auction. More precisely, it is determined by the number $f(v)$ with a. Hence, we can first work on the probability distribution on $[0, w]$ for $f(v)$ and return back to $\tau(s)$ at the end of Section 5.5.
Recall that writing $X_i = \lfloor v_i(1) \rfloor$ and $Y_i = \lfloor v_i(0) \rfloor$, we have

$$\begin{aligned} M^T(v).A : W &\to \mathbb{B} \\ i &\mapsto (X_i \notin \{ Y_i \mid j \neq i \}). \end{aligned}$$

Given $Y = (Y_0, \cdots, Y_{w-1}) \in [0, w)^w$, there are $w - \#\{ Y_j \mid j \neq i \}$ choices for $X_i \notin \{ Y_j \mid j \neq i \}$. Therefore, the conditional probability of $X_i \notin \{ Y_j \mid j \neq i \}$ given Y is:

$$P_{i|Y} = \frac{w - \#\{ Y_j \mid j \neq i \}}{w}. \tag{5.3.1}$$

Hence, the probability that the cardinality $f(v) = w' \in [0, w]$ is:

$$\begin{array}{ll} & P\left(f(v) = w'\right) \\ = & \text{from the Rule of Conditional Probability} \\ & \sum_{Y \in [0,w)^w} P\left(f(v) = w' \mid Y\right) P(Y) \\ = & \text{factorizing } P(Y) \text{ and expanding } P\left(f(v) = w' \mid Y\right) \\ & \frac{1}{w^w} \sum_{Y \in [0,w)^w} \sum_{A \subseteq [0,w), \#A = w'} \left(\prod_{i \in A} P_{i|Y}\right) \left(\prod_{j \in [0,w) \setminus A} (1 - P_{j|Y})\right) \\ = & \text{factorizing the } \tfrac{1}{w}\text{'s from the } P_{k|Y}\text{'s} \\ & \frac{1}{w^{2w}} \sum_{Y \in [0,w)^w} \sum_{A \subseteq [0,w), \#A = w'} g(A, Y) \end{array}$$

where

$$g(A, Y) := \left(\prod_{i \in A} (w - \#\{ Y_k \mid k \neq i \})\right) \left(\prod_{j \in [0,w) \setminus A} (\#\{ Y_k \mid k \neq j \})\right).$$

Note that each set A in the expansion of $P\left(f(v) = w' \mid Y\right)$ corresponds to a possible allocation in $\mathcal{A}$, hence the notation.
Using this definition of $P(f(v) = w')$, we can obtain an expression for $\tau(s)(s')$ for all $s' : TState$. Nevertheless, the two enumerations ($Y : [0, w)^w$ and $A \subseteq [0, w)$) in this formula mystify the behaviour of $\tau(s)$. Fortunately, they can be significantly reduced as we shall see in the next two sections.

5.4 Independent of the set A

Note that we have two independent summations in the last expression for $P(f(v) = w')$ given in Section 5.3. Hence by changing the summation order, we also have:

$$P\left(f(v) = w'\right) = \frac{1}{w^{2w}} \sum_{A \subseteq [0,w), \# A = w'} \sum_{Y \in [0,w)^w} g(A, Y). \tag{5.4.1}$$

Observe that if A^0 and A^1 are subsets of $[0, w)$ that are of the same size and $Y^0 : [0, w)^w$ is a permutation of $Y^1 : [0, w)^w$ such that the components of Y^1 at coordinates in A^1 are exactly the components of Y^0 at coordinates in A^0, then the pairs (A^0, Y^0) and (A^1, Y^1) have the same image by g. We formally prove this in the following lemma.

Lemma 5.4.1 *Let $\sigma : [0, w) \rightarrowtail [o, w)$ be a bijection. Then, there exists a bijection φ_σ on $[0, w)^w$ such that for all $Y \in [0, w)^w$ and for all $A \subseteq [0, w)$ with $\#A = w'$, we have:*

$$g(\sigma^{-1}(A), \varphi_\sigma(Y)) = g(A, Y).$$

***Proof*:** Define

$$\begin{aligned} \varphi_\sigma : [0, w)^w &\to [0, w)^w \\ Y &\mapsto \varphi_\sigma(Y) = (Y_{\sigma(0)}, \cdots, Y_{\sigma(w-1)}). \end{aligned}$$

Let $Y \in [0, w)^w$ and $A \subseteq [0, w)$. Then,

$g(\sigma^{-1}(A), \varphi_\sigma(Y))$

$=$ by the definition of g

$\prod_{i \in \sigma^{-1}(A)}(w - \#\{\varphi_\sigma(Y)_k \mid k \neq i\}) \prod_{j \in [0,w) \setminus \sigma^{-1}(A)}(\#\{\varphi_\sigma(Y)_k \mid k \neq j\})$

$=$ by the definition of φ_σ

$\prod_{i \in \sigma^{-1}(A)}(w - \#\{Y_{\sigma(k)} \mid \sigma(k) \neq \sigma(i)\}) \prod_{j \in [0,w) \setminus \sigma^{-1}(A)}(\#\{Y_{\sigma(k)} \mid \sigma(k) \neq \sigma(j)\})$

$=$ since σ is a bijection

$\prod_{i \in A}(w - \#\{Y_k \mid k \neq i\}) \prod_{j \in [0,w) \setminus A}(\#\{Y_k \mid k \neq j\})$

$=$ by the definition of g,

$g(A, Y)$.

□

As a corollary to Lemma 5.4.1, the following proposition shows that the inner most summation in Equation (5.4.1) is constant on A.

Proposition 5.4.2 *Let $A_0 = [0, w')$. Then, for all $A \subseteq [0, w)$ with $\#A = w'$,*

$$\sum_{Y \in [0,w)^w} g(A, Y) = \sum_{Y \in [0,w)^w} g(A_0, Y).$$

***Proof*:** For all $A \subseteq [0, w)$ with $\#A = w'$, there exists a bijection

$$\sigma : [0, w) \rightarrowtail [0, w)$$

such that $\sigma(A) = A_0$. The result follows from Lemma 5.4.1. □

It follows from Proposition 5.4.2 that

$$P\left(f(v) = w'\right) = \frac{1}{w^{2w}} \binom{w}{w'} \sum_{Y \in [0,w)^w} \left(\prod_{i=0}^{w'-1} (w - \#\{Y_k \mid k \neq i\}) \prod_{j=w'}^{w-1} (\#\{Y_k \mid k \neq j\}) \right).$$

Remark 5.4.3 *Distributing the binomial coefficient to the terms in the summation does not give the conditional probability of $f(v) = w'$ given Y. For instance take $w = 4$, $Y = (0, 1, 0, 0)$ and $w' = 2$. We have*

$$\binom{w}{w'} g(A_0, Y) = \frac{9}{16}$$

while

$$\sum_{A \subseteq [0,w), \#A = w'} g(A, Y) = \frac{3}{8}.$$

From now on, $g(Y)$ denotes $g(A_0, Y)$ for all $Y \in [0, w)^w$.

5.5 Equivalence Relation on $[0, w)^2$

We now reduce the summation over $[0, w)^2$ through an equivalence relation. The following lemma tells us which one to consider.

Lemma 5.5.1 *Let $\sigma : [0, w) \rightarrowtail [0, w)$ be a bijection and define:*

$$\begin{aligned} \psi_\sigma : [0, w)^w &\to [0, w)^w \\ Y &\mapsto \psi_\sigma(Y) = (\sigma(Y_0), \cdots, \sigma(Y_{w-1})). \end{aligned}$$

Then, $g(Y) = g(\psi_\sigma(Y))$ for all $Y \in [0, w)^w$.

***Proof*:** For all $i \in [0, w)$,

$$\#\{ Y_k \mid k \neq i\} = \#\{\sigma(Y_k) \mid k \neq i\} = \#\{\psi_\sigma(Y)_k \mid k \neq i\}.$$

□

Lemma 5.5.1 simply says that the image of Y by g does not depend on the representation of its components. Hence, if Y^0 and Y^1 are such that whenever we find the same element at two coordinates in Y^0, we do so at these two coordinates in Y^1, then Y^0 and Y^1 are equivalent with regard to their image by g. Define the equivalence relation

$$\backsim := \{(Y^0, Y^1) \in [0, w)^{2w} \mid \exists \sigma : [0, w) \rightarrowtail [0, w) \bullet Y^1 = \psi_\sigma(Y^0)\}$$

on $[0, w)^w$. Indeed, $\backsim$ is reflexive (take $id_{[0,w)}$), symmetric (take σ^{-1}) and transitive (take the composition).
Let $Y^0 \in [0, w)^w$. Then, every injection of $\{ Y^0_k \mid k \in [0, w)\}$ into $[0, w)$ corresponds to a unique

$$Y^1 \in [Y^0] := \{ Y^2 \in [0, w)^w \mid Y^0 \backsim Y^2\}.$$

Therefore, the equivalence class $[Y^0] \in [0, w)^w / \backsim$, represented by its element $Y^0 \in [0, w)^w$ with $\#\{ Y^0_k \mid k \in [0, w)\} = n$ has $n!\binom{w}{n}$ elements.
Besides, any Y^0 and $Y^1 \in [0, w)^w$ such that

$$\#\{ Y^0_k \mid k \in [0, w)\} \neq \#\{ Y^1_k \mid k \in [0, w)\}$$

are not equivalent. Therefore, we can label the classes by the common cardinality

$$\#\{ Y_k \mid k \in [0, w)\} = n \in [1, w]$$

of their elements. Moreover, we know that each class which has the label n corresponds to a unique mapping of $[0, w)$ onto $[0, n)$, which means to a unique partition of $[0, w)$ into n parts. (Hence, there are $\mathcal{S}(w, n)$, with S the Stirling number of the second kind, classes in the group [26]).
It follows that

$$\begin{aligned}
& P\left(f(v) = w'\right) \\
= \quad & \text{from the last expression given in Section 5.4.2} \\
& \tfrac{1}{w^{2w}}\tbinom{w}{w'} \textstyle\sum_{Y \in [0,w)^w} g(Y) \\
= \quad & \text{summation over the equivalence classes} \\
& \tfrac{1}{w^{2w}}\tbinom{w}{w'} \textstyle\sum_{[Y] \in [0,w)^w/\backsim} \#[Y] g(Y) \\
= \quad & \text{using the labels} \\
& \tfrac{1}{w^{2w}}\tbinom{w}{w'} \textstyle\sum_{n=1}^{w} n!\tbinom{w}{n} \sum_{P \in Part(w,n)} \hat{g}(P),
\end{aligned}$$

where $Part(w, n)$ is the set of all partitions of $[0, w)$ into n parts and

$$\hat{g}(P) = \prod_{E \in P} (w - (n - 1 + \mu(E)))^{\#\{x \in E | x < w'\}} (n - 1 + \mu(E))^{\#\{x \in E | x \geq w'\}}$$

with $\mu(E) = 0$ if $\#E = 1$ and $\mu(E) = 1$ otherwise.
Now, observe that $\hat{g}(P)$ does not depend on the actual elements of $[0, w)$ in each part $E \in P$. It rather depends on two numbers:

$$\rho_1 = \#\{x \in [0, w) \mid \exists\, E \in P \bullet \#E > 1 \wedge x \in E \wedge x < w'\}, \tag{5.5.1}$$
$$\rho_2 = \#\{x \in [0, w) \mid \exists\, E \in P \bullet \#E > 1 \wedge x \in E \wedge x \geq w'\}. \tag{5.5.2}$$

Fixed $n \in [1, w)$, $\rho_1 \leq w'$ and $\rho_2 \leq w - w'$, a $P \in Part(w, n)$ that satisfies 5.5.1 and 5.5.2 contains $w - (\rho_1 + \rho_2) \geq 0$ singletons and has

$$\begin{aligned}\hat{g}(P) &= \prod_{E \in P} (w - (n - 1 + \mu(E)))^{\#\{x \in E | x < w'\}} (n - 1 + \mu(E))^{\#\{x \in E | x \geq w'\}} \\ &= (w - n + 1)^{w' - \rho_1} (w - n)^{\rho_1} (n - 1)^{w - w' - \rho_2} n^{\rho_2} \\ &=: h(\rho_1, \rho_1 + \rho_2, w, n).\end{aligned}$$

Besides, the number of such partitions is

$$\binom{w'}{\rho_1} \binom{w - w'}{\rho_2} \mathcal{S}^*(\rho_1 + \rho_2, n - w + \rho_1 + \rho_2),$$

where $\mathcal{S}^*(\rho_1 + \rho_2, n - w + \rho_1 + \rho_2)$ is the number of ways to distribute the $\rho_1 + \rho_2$ elements into $n - w + \rho_1 + \rho_2$ subsets of cardinality > 1.
Before we can make use of that observation, let us examine the domains of ρ_1 and ρ_2. Firstly, we already know that

$$0 \leq \rho_1 \leq w' \text{ and } 0 \leq \rho_2 \leq w - w'.$$

Secondly, since each of the $n - w + \rho_1 + \rho_2$ must have at least two elements,

$$0 \leq n - w + \rho_1 + \rho_2 \leq \frac{\rho_1 + \rho_2}{2},$$

which implies

$$\frac{\rho_1 + \rho_2}{2} \leq w - n.$$

In addition, since the number of singletons must be strictly smaller than the size $n < w$ of the partition, we have $w - \rho_1 - \rho_2 < n$. Hence

$$w - n < \rho_1 + \rho_2 \leq min(w, 2(w - n)),$$

for $n \in [1, w)$. By considering the sum $\rho := \rho_1 + \rho_2$, we have

$$0 \leq \rho - \rho_1 \leq w - w',$$

which means

$$w' - w + \rho \leq \rho_1 \leq \rho,$$

and obtain the domains of ρ, ρ_1:

$$w - n + 1 \leq \rho \leq min(w, 2(w-n))$$

and

$$max(0, w' - w + \rho) \leq \rho_1 \leq min(\rho, w'),$$

for $n \in [1, w)$.
Since there is only one partition of $[0, w)$ into w parts, namely the one with n singletons, the probability $P(f(v) = w')$ becomes

$$P(f(v) = w') = \frac{1}{w^{2w}}\binom{w}{w'}\left[w!(w-1)^{w-w'} + \sum_{n=1}^{w-1} n!\binom{w}{n} \sum_{\rho=w-n+1}^{min(w,2(w-n))} \sum_{\rho_1=max(0,w'-w+\rho)}^{min(\rho,w')} \binom{w'}{\rho_1}\binom{w-w'}{\rho-\rho_1}\mathcal{S}^*(\rho, n-w+\rho)h(\rho_1, \rho, w, n)\right].$$

Following [26], the class $\mathcal{S}^{(C,N)}$ of set partitions with block sizes in C and number of blocks in N has the generating function

$$\mathcal{S}^{(C,N)}(z) = \nu(\zeta(z)),$$

where

$$\zeta(z) = \sum_{c \in C} \frac{z^c}{c!} \text{ and } \nu(z) = \sum_{n \in N} \frac{z^n}{n!}.$$

Therefore, by taking $C = [2, \infty)$ and $N = \{n - w + \rho\}$, we can compute $\mathcal{S}^*(\rho, n - w + \rho)$ using the generating function:

$$\mathcal{S}(z) = \frac{(e^z - 1 - z)^{n-w+\rho}}{(n-w+\rho)!}.$$

To summarize, we have the following proposition.

Proposition 5.5.2 *Let $w : \mathbb{N}$ be the number of bidders and let $w' : [0, w]$. Then, the probability that the chosen valuation profile v is such that M^T allocates 1 to w' players, is given by*

$$P(f(v) = w') = \frac{1}{w^{2w}}\binom{w}{w'}\left[w!(w-1)^{w-w'} + \sum_{n=1}^{w-1} n!\binom{w}{n} \sum_{\rho=w-n+1}^{min(w,2(w-n))} \sum_{\rho_1=max(0,w'-w+\rho)}^{min(\rho,w')} \binom{w'}{\rho_1}\binom{w-w'}{\rho-\rho_1}\mathcal{S}^*(\rho, n-w+\rho)h(\rho_1, \rho, w, n)\right],$$

where

$$h(\rho_1, \rho, w, n) := (w - n + 1)^{w' - \rho_1}(w - n)^{\rho_1}(n - 1)^{w - w' - \rho + \rho_1} n^{\rho - \rho_1},$$

and

$$\mathcal{S}^*(\rho, n - w + \rho) = \frac{d^\rho}{dz^\rho}\left(\frac{(e^z - 1 - z)^{n-w+\rho}}{(n - w + \rho)!}\right).$$

Coming back to the distribution $\tau(s)$, consider a state $s' : TState$.
If $s'.a > s.a$, then it is clear that $\tau(s)(s') = 0$. If $s' = \mathbf{0}$, it means that the allocation profile yielded exactly $s.a$ winning bidders. Hence,

$$\tau(s)(\mathbf{0}) = P(f(v) = s.a).$$

Now, following the two cases explained in Section 5.2, $s'.a \in (0, s.a)$ means that the cardinality $f(v) \in (0, s.a)$ and the number of players left for the next auction is $s'.w = s.w - f(v)$. In that case, we have

$$\tau(s)(s') = P(f(v) = s.w - s'.w).$$

If $s'.a = s.a$, then either $f(v) = 0$ (which implies $s'.w = s.w$) or $f(v) > s.a$. Hence in this case, if $s'.w = s.w$, then

$$\tau(s)(s') = P(f(v) = 0) + P(f(v) = s.w)$$

and if $s'.w < s.w$, then

$$\tau(s)(s') = P(f(v) = s'.w).$$

5.6 Tie Breaking for a Single Prize

Suppose that there is only one prize ($s.a = 1$) and let $s' : TState$. Then

$$\tau(s)(s') = \begin{cases} P(f(v) = 1) & \text{if } s' = \mathbf{0} \\ P(f(v) = s'.w) & \text{if } s'.a = 1 \wedge s'.w < s.w \\ P(f(v) = 0) + P(f(v) = s.w) & \text{if } s'.a = 1 \wedge s'.w = s.w \\ 0 & \text{otherwise.} \end{cases}$$

Using the formula presented in Proposition 5.5.2, we obtain the distributions plotted in Figure 5.1 as examples. Each curve shows the image by τ of some state $s : TState$ with $s.a = 1$, restricted on $\{s : TState \mid s.a \leq 1\}$ since outside this domain, $\tau(s)$ is constant equal to zero.

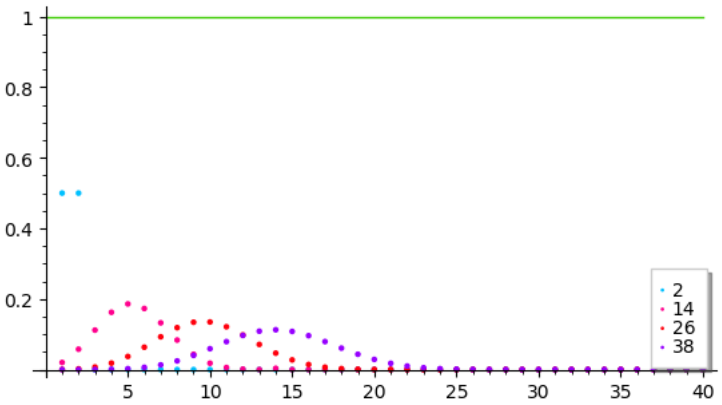


Figure 5.1: Horizontal axis $s'.w$, vertical axis $\tau(s)(s')$ for $s.a = 1$ and $s.w = 2, 14, 26, 38$.

As mentioned in Section 5.2, we run the program τ until the state $\mathbf{0}$ is reached. By using the weakest precondition $wp.(h \fatsemi h').\beta$ for $h, h : \mathcal{HS}$ as defined in [25] with $\mathcal{S} = TState$ and $\beta := (s = \mathbf{0})$, or by building a stochastic matrix with $\tau(s)(s')$, we can work on the probability for reaching $\mathbf{0}$ after k iterations. As shown in Figure 5.2, this probability increases with $k : \mathbb{N}^*$. Moreover, the number $s.w$ of players in the initial state s does not significantly affect its convergence to 1. In Figure 5.2, we see that the ties are broken with high probability after only 6 iterations, even for $s.w = 38$.

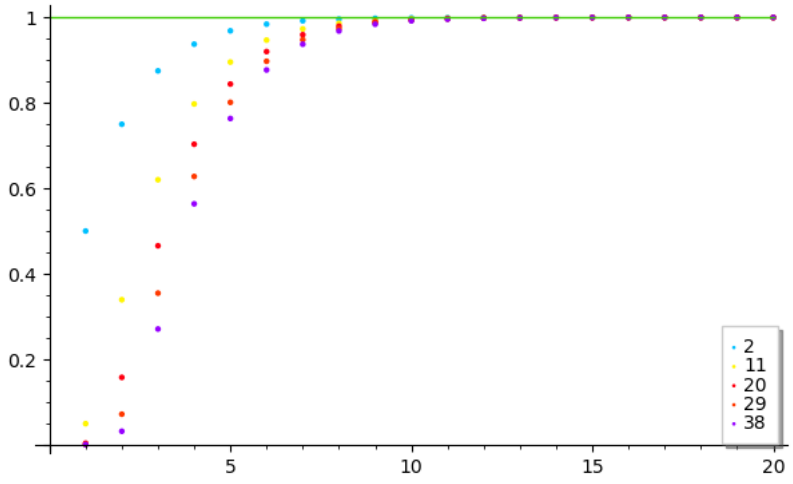


Figure 5.2: Horizontal axis the number k of iterations, vertical axis $\tau^k(s)(\mathbf{0})$ for $s.a = 1$ and $s.w = 2, 14, 26, 38$.

5.7 Chapter Summary

In this chapter, we have presented a mechanism for tie breaking which we have used with the bid collection rules $\mathcal{R}_S$ for distributed sealed-bid auctions. The resulting tie-breaking protocol is symmetric so that it can be used for *Leader Election* without a specific network topology (unlike, for instance, *Herman' s Ring* [11]).
We have given a simplified explicit formula for the probability distribution over the state space which the protocol yields for a given initial state. We have seen by means of simulations that the protocol breaks ties with high probability in only few iterations, independently of the initial number of players, for a single prize. As mentioned in Section 4.6, each iteration can be done in 3 rounds if the system is synchronous. Also in each iteration, a player needs to send $2b$ messages to make the only one required bid.
Since the players may leave the competition in different iterations and the winner is one of those who stays until the end, the number of messages a player sends until leaving the competition is at most the same as the winner's.

Chapter 6

Conclusion

In this document, we have presented a framework which allows studies of auction mechanisms to be centralized (Chapter 2). We have studied two mechanism spaces for compact (with respect to a metric, given in that chapter) and convex valuation spaces and gave some of their properties (Chapter 3). The results we have obtained exposed the relative simplicity of some truthful mechanisms.
We have shown how to distribute a sealed-bid auction in a way that auctioneers are not needed as every participant can compute the outcome independently (Chapter 4). We have gained that independence by forfeiting the privacy of bids at the end of the auction (which as mentioned in Chapter 1, is the focus of [12] and [13]). However, from Proposition 4.5.3, the bidders don't know each others' bids until they no longer can bid and the bids can be made anonymous.
Finally, we have proposed a tie-breaking mechanism for distributed sealed-bid auctions which, as a protocol, can also be used for Leader Election without a specific network topology (Chapter 5). We have given an explicit formula for the probability distribution over the state space, which the protocol yields for a given initial state. Nevertheless, an average case analysis of the protocol should be part of a future work.
Besides, it would be interesting to study Nash Equilibrium mechanisms the same way as for $\mathcal{M}^u(\mathcal{V})$. Also an in-depth analysis of distributed English auctions would be of great importance as this is the most common form.

Bibliography

[1] Heaton, L.: *A Brief History of Mathematical Thought*. Oxford University Press, 2017.

[2] Osborne, M.J. and Rubinstein, A.: *A Course in Game Theory*. MIT press, 1994.

[3] Myerson, R.B.: Optimal auction design. *Mathematics of Operations Research*, vol. 6, no. 1, pp. 58–73, 1981.

[4] Khan, A.M., Vilaça, X., Rodrigues, L. and Freitag, F.: A distributed auctioneer for resource allocation in decentralized systems. In: *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, pp. 201–210. IEEE, 2016.

[5] Jap, S.D.: An exploratory study of the introduction of online reverse auctions. *Journal of Marketing*, vol. 67, no. 3, pp. 96–107, 2003.

[6] Nisan, N.: Algorithmic mechanism design: Through the lens of multiunit auctions. In: *Handbook of Game Theory with Economic Applications*, vol. 4, pp. 477–515. Elsevier, 2015.

[7] Papadimitriou, C., Schapira, M. and Singer, Y.: On the hardness of being truthful. In: *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pp. 250–259. IEEE, 2008.

[8] Fagin, R., Moses, Y., Halpern, J.Y. and Vardi, M.Y.: *Reasoning about Knowledge*. MIT press, 2003.

[9] Blum, M.: Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, vol. 15, no. 1, pp. 23–27, 1983.

[10] Attiya, H. and Welch, J.: *Distributed Computing: Fundamentals, Simulations, and Advanced Topics*, vol. 19. John Wiley & Sons, 2004.

[11] McIver, A. and Morgan, C.: An elementary proof that herman's ring is $\theta(n^2)$. *Information Processing Letters*, vol. 94, no. 2, pp. 79–84, 2005.

[12] Brandt, F.: Fully private auctions in a constant number of rounds. In: *International Conference on Financial Cryptography*, pp. 223–238. Springer, 2003.

[13] Kulshrestha, A., Rampuria, A., Denton, M. and Sreenivas, A.: Cryptographically secure multiparty computation and distributed auctions using homomorphic encryption. *Cryptography*, vol. 1, no. 3, p. 25, 2017.

[14] Spivey, J.M.: *The Z Notation*. 2nd edn. Prentice-Hall International, 1992.

[15] Duke, R. and Rose, G.: *Formal Object-Oriented Specification using Object-Z*. Macmillan, 2000.

[16] Vickrey, W.: Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance*, vol. 16, no. 1, pp. 8–37, 1961.

[17] Klemperer, P.: Auction theory: A guide to the literature. *Journal of Economic Surveys*, vol. 13, no. 3, pp. 227–286, 1999.

[18] De Vries, S. and Vohra, R.V.: Combinatorial auctions: A survey. *INFORMS Journal on Computing*, vol. 15, no. 3, pp. 284–309, 2003.

[19] Milgrom, P.R. and Weber, R.J.: A theory of auctions and competitive bidding. *Econometrica: Journal of the Econometric Society*, pp. 1089–1122, 1982.

[20] Gneezy, U. and Smorodinsky, R.: All-pay auctions-an experimental study. *Journal of Economic Behavior & Organization*, vol. 61, no. 2, pp. 255–275, 2006.

[21] Friedman, L.: A competitive-bidding strategy. *Operations Research*, vol. 4, no. 1, pp. 104–112, 1956.

[22] von Neumann, J.: Zur theorie der gesellschaftsspiele. *Mathematische Annalen*, vol. 100, no. 1, pp. 295–320, 1928.

[23] Nash, J.: Non-cooperative games. *Annals of Mathematics*, pp. 286–295, 1951.

[24] Klemperer, P.: What really matters in auction design. *Journal of Economic Perspectives*, vol. 16, no. 1, pp. 169–189, 2002.

[25] Morgan, C., McIver, A. and Seidel, K.: Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 18, no. 3, pp. 325–353, 1996.

[26] Flajolet, P. and Sedgewick, R.: *Analytic Combinatorics*. Cambridge University Press, 2009.